Universidade Federal do ABC

Segurança de Redes

Aula 01
Introdução

Prof. João Henrique Kleinschmidt

Santo André, setembro de 2019

Roteiro

PARTE I – Apresentação da Disciplina

PARTE II – Introdução à Segurança de Redes

Apresentação do Professor

- Prof. João Henrique Kleinschmidt

- Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas (CECS)
  - E-mail: joao.kleinschmidt@ufabc.edu.br
  - Web

    http://professor.ufabc.edu.br/~joao.kleinschmidt

Metodologia

- 4 horas-aulas semanais
  - Aulas teóricas (3 h)
  - Aulas práticas (1 h)

- Aulas expositivas
- Exercícios em sala (teoria)
- Uso de ferramentas de segurança (lab.)
- Atividades e exercícios extra-classe

Avaliação

- Provas: 60%
  - Prova P1 – 30% - Data: 31/10
  - Prova P2 – 30% - Data: 10/12
- Exercícios de teoria: 10%
- Laboratórios: 30%

- Prova substitutiva para quem faltar P1 ou P2 (com justificativa)
- Prova de recuperação de toda a matéria para aluno que ficar com D ou F.

Cálculo do Conceito Final

- Relação Nota – Conceito
  - 9-10 = A
  - 7-9 = B
  - 6-7 = C
  - 5-6 = D
  - <5 = F

Bibliografia

- Notas de aula – Disponíveis na página
  - http://professor.ufabc.edu.br/~joao.kleinschmidt
- Livros
  - TANENBAUM, Andrew S. Redes de computadores. 4.ed. Rio de Janeiro: Elsevier, 2003.
  - W. STALLINGS, “Criptografia e Segurança de Redes – Princípios e Práticas”, Prentice Hall, 4a Ed., 2007.
  - Seg
  - W. STALLINGS, “Network Security Essentials: Applications and Standards”, Prentice Hall, 3a Ed., 2006.
  - M. RHODES–OUSLEY, R. BRAGG, K. STRASSBERG, “Network Security: The Complete Reference”, McGraw-Hill; 1a Ed., 2003.
  - NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes em Ambientes Cooperativos. Novatec, 2007. COLE, E. Network Security Bible. 2. ed. Wiley, 2009.
- Sites da Internet e ferramentas de segurança

Conteúdo

Introdução à Segurança da Informação; Gerenciamento da Segurança: política de segurança, análise de riscos e auditoria; Mecanismos Criptográficos de Segurança; Criptografia de Chaves Públicas: Uso em Certificação Digital; Infraestrutura de chaves públicas; Mecanismo de Autenticação e controle de acesso. Negação de serviço (DoS). Firewalls, sistemas de prevenção e detecção de intrusão. Segurança em software. Segurança na Internet.

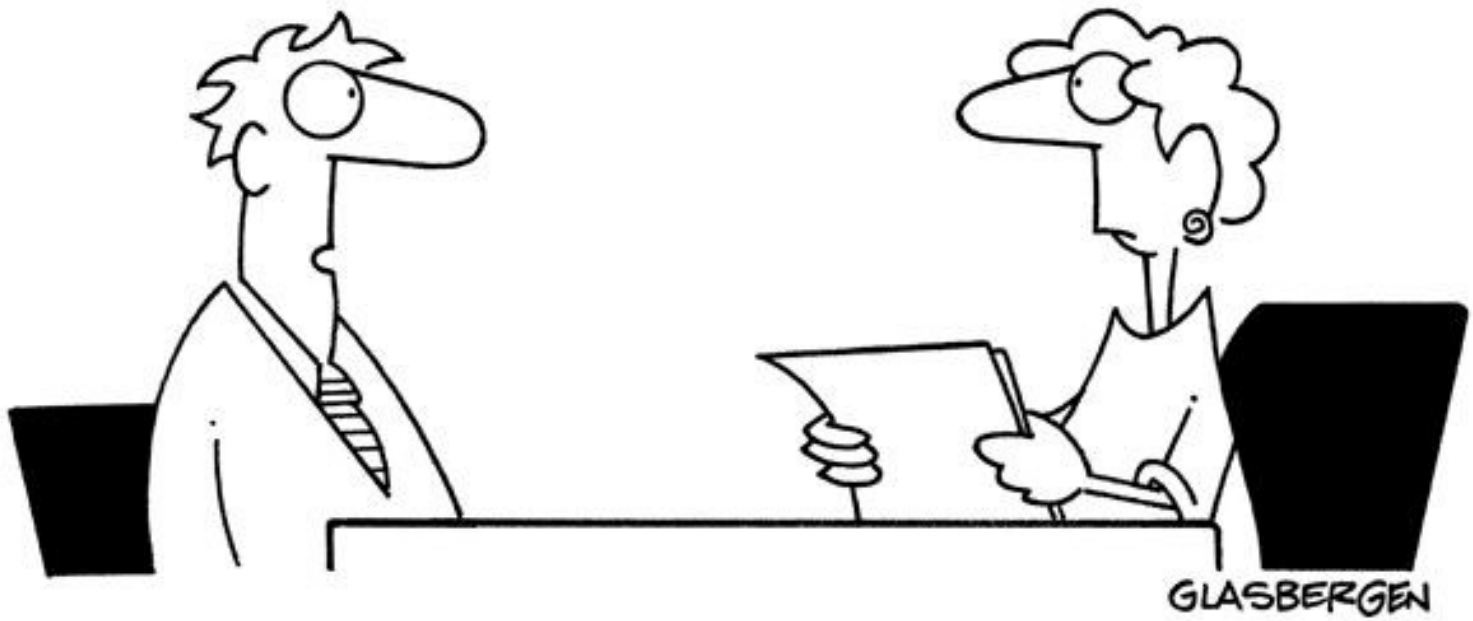
*Recomendação: Redes de Computadores

Motivação

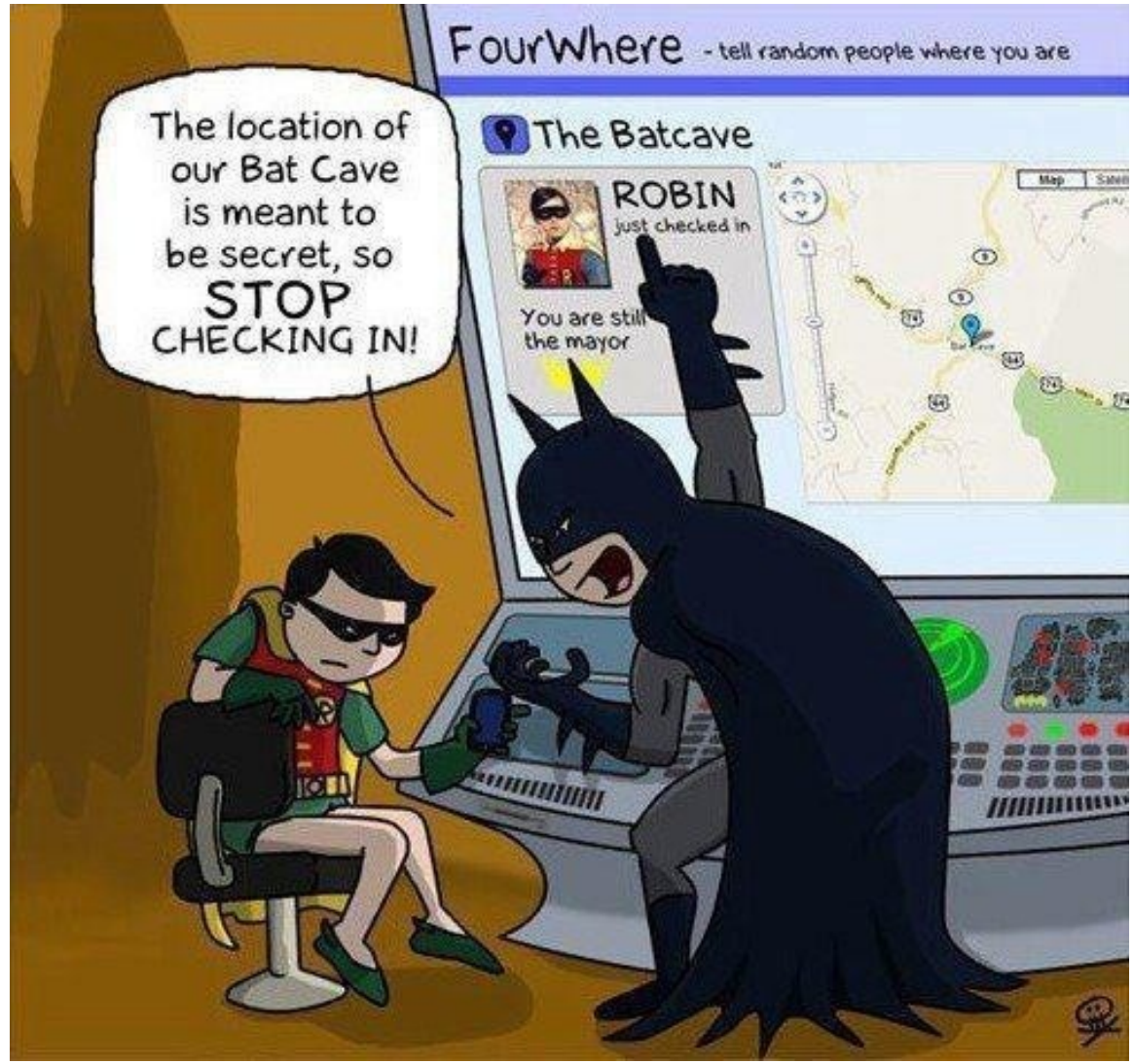
-Casos recentes

-Novo golpe pelo WhatsApp rouba contas de quem faz vendas na internet
- Cibercrime roubou 2 milhões de cartões de crédito no Brasil com malware
- Segundo fator de autenticação bloqueia 100% de hacks via bot, diz Google
- Youtuber mostra como burlar a biometria do OnePlus 7 Pro usando apenas cola
- Julian Assange, do WikiLeaks, é condenado por violar Lei de Espionagem
- Funcionários do Snapchat espionaram fotos e mensagens de usuários
- Notebook infectado com WannaCry vale US$ 1 milhão em leilão de arte

Notícias de Maio de 2019 (Fonte: www.tecmundo.com.br)



"For the sake of information security, everything on my résumé is false."


FourWhere - tell random people where you are
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!
The Batcave
ROBIN
just checked in
You are still the mayor


NAH, I'M NOT WORRIED ABOUT CLOUD SECURITY. MY STORED DATA IS SO DISORGANIZED THEY'D NEVER BE ABLE TO FIND ANYTHING!
© D.Fletcher for CloudTweaks.com

Parte II

Introdução à Segurança da Informação

Segurança da Informação

- "Segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento".

Motivação

- Segurança não é algo binário
- Não existe rede totalmente segura
- Pode-se falar em:
  - Mais segurança
  - Menos segurança
- Portanto: gerenciamento de SI deve ser constante

Informação

- Informação pode existir de muitas formas:
  - Impressa ou escrita em papel
  - Armazenada eletronicamente
  - Transmitida pelo correio ou meios eletrônicos
  - Mostrada em filmes
  - Falada em conversas
- Sempre deve ser protegida adequadamente

Segurança da Informação

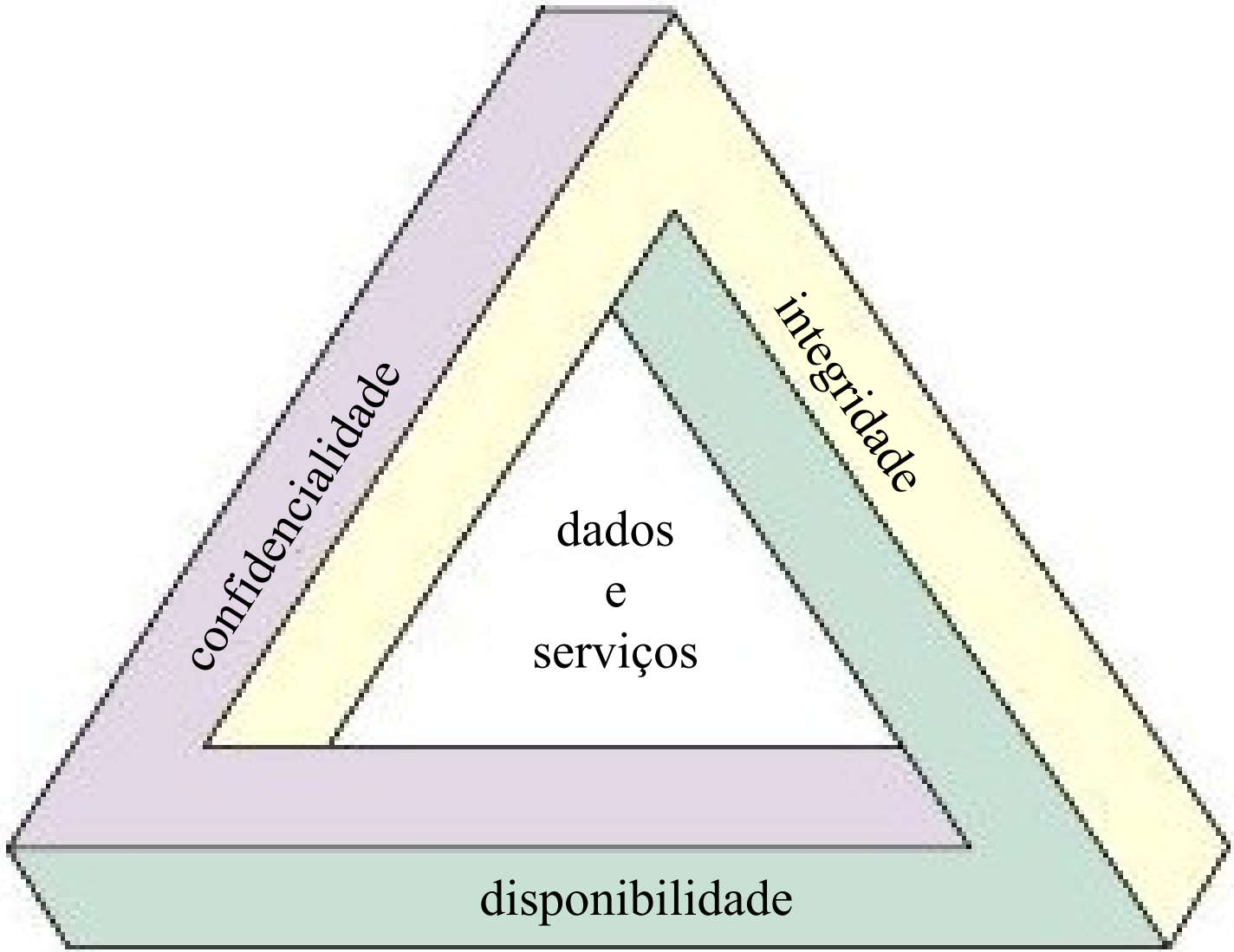
- Preservação de:

Confidencialidade

Integridade

Disponibilidade

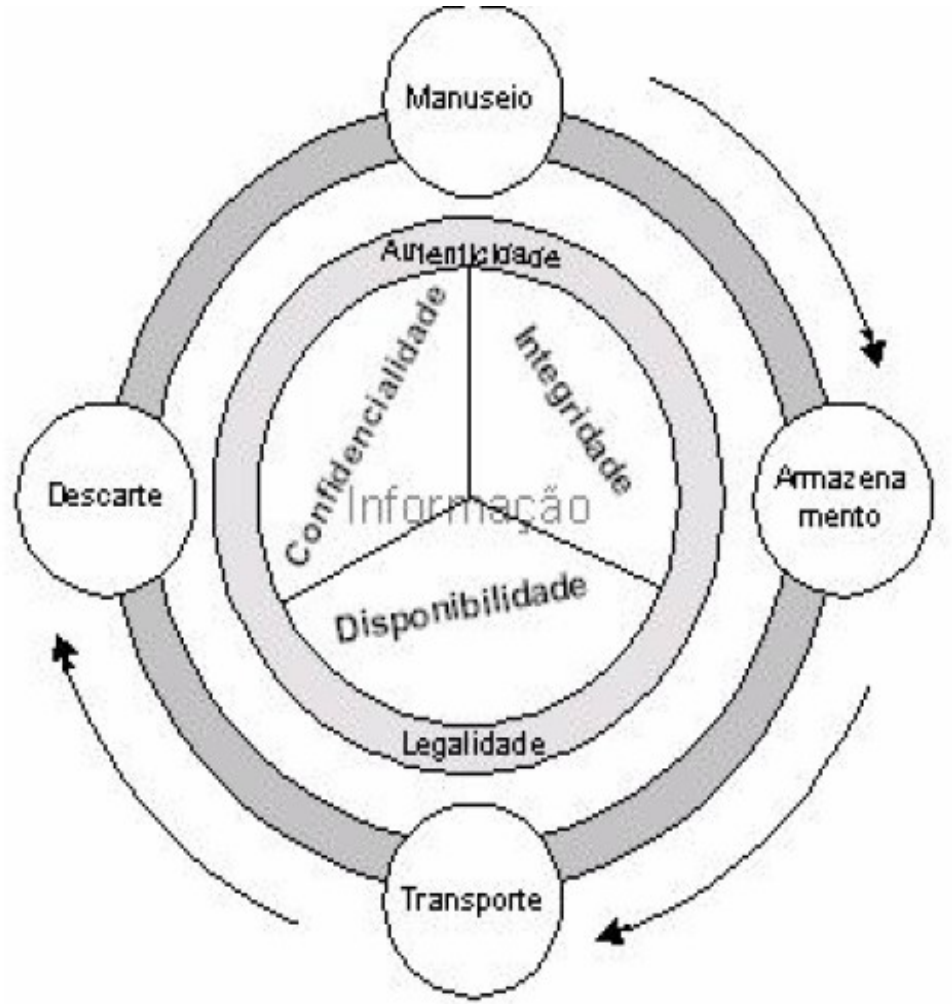
Segurança da Informação



Sistema seguro

- **Confidencialidade** – A informação somente pode ser acessada por pessoas explicitamente autorizadas; é a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo.
- **Disponibilidade** – A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;
- **Integridade** – A informação deve ser retornada em sua forma original no momento em que foi armazenada.

Ciclo de vida da informação



Classificação das informações

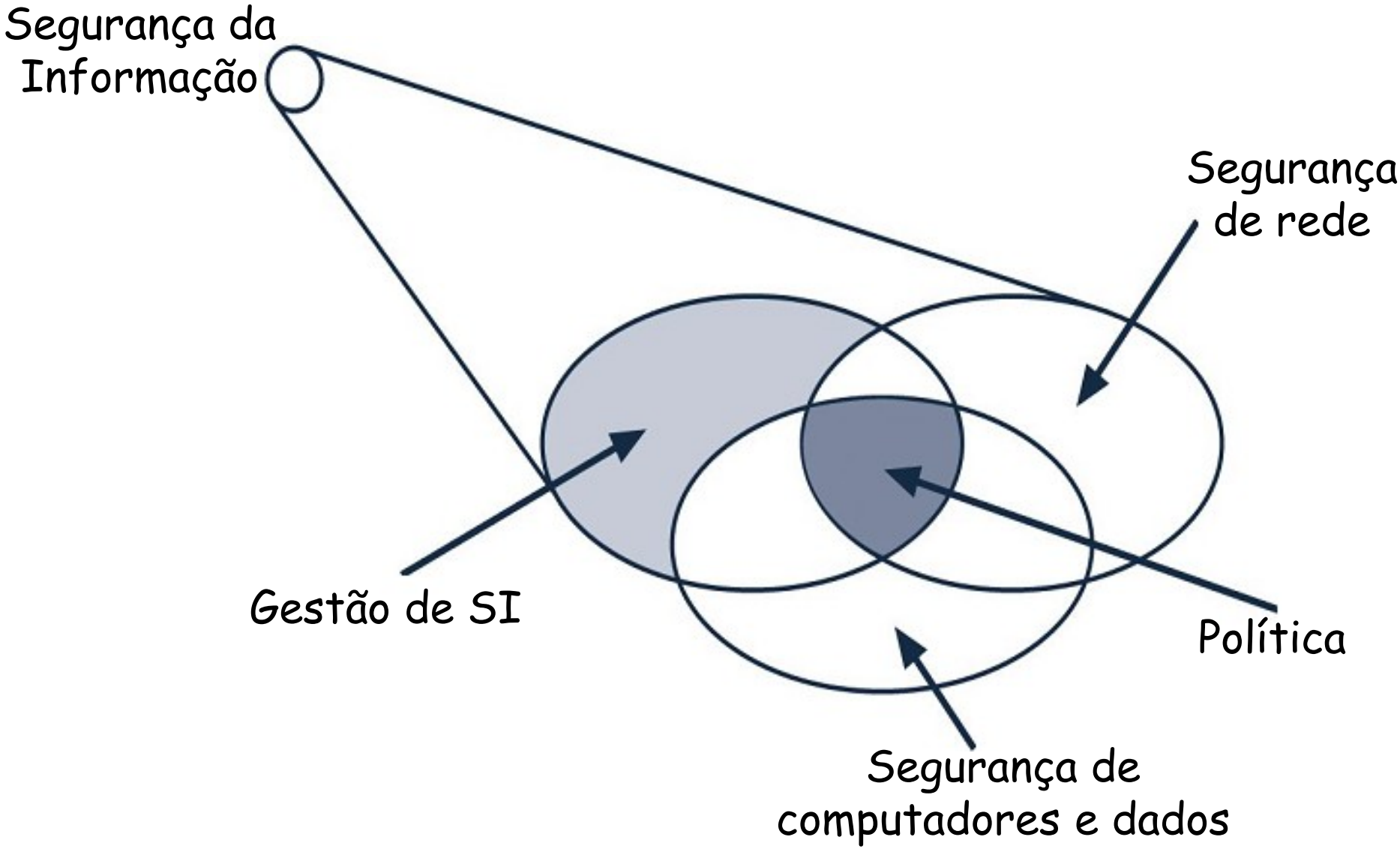
- **Pública** – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa;
- **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias;
- **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras;
- **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas.

Esta é apenas uma possível classificação!!!

Segurança: Objetivos expandidos

- Confidencialidade
  - Garantia de que apenas pessoas autorizadas tenham acesso a informação
- Integridade
  - Manutenção do valor e do estado da informação; Proteção contra alterações não autorizadas
- Disponibilidade
  - Garantia que a informação estará disponível quando necessária
- Irretratabilidade (ou não-repúdio)
  - Habilidade de provar que o remetente realmente enviou ou é autor de uma informação
- Autenticação
  - A prova da identidade para concessão da autorização

Componentes da SI



Como a SI pode ser obtida?

- Implementando **CONTROLES,** para garantir que os objetivos de segurança sejam alcançados

Políticas

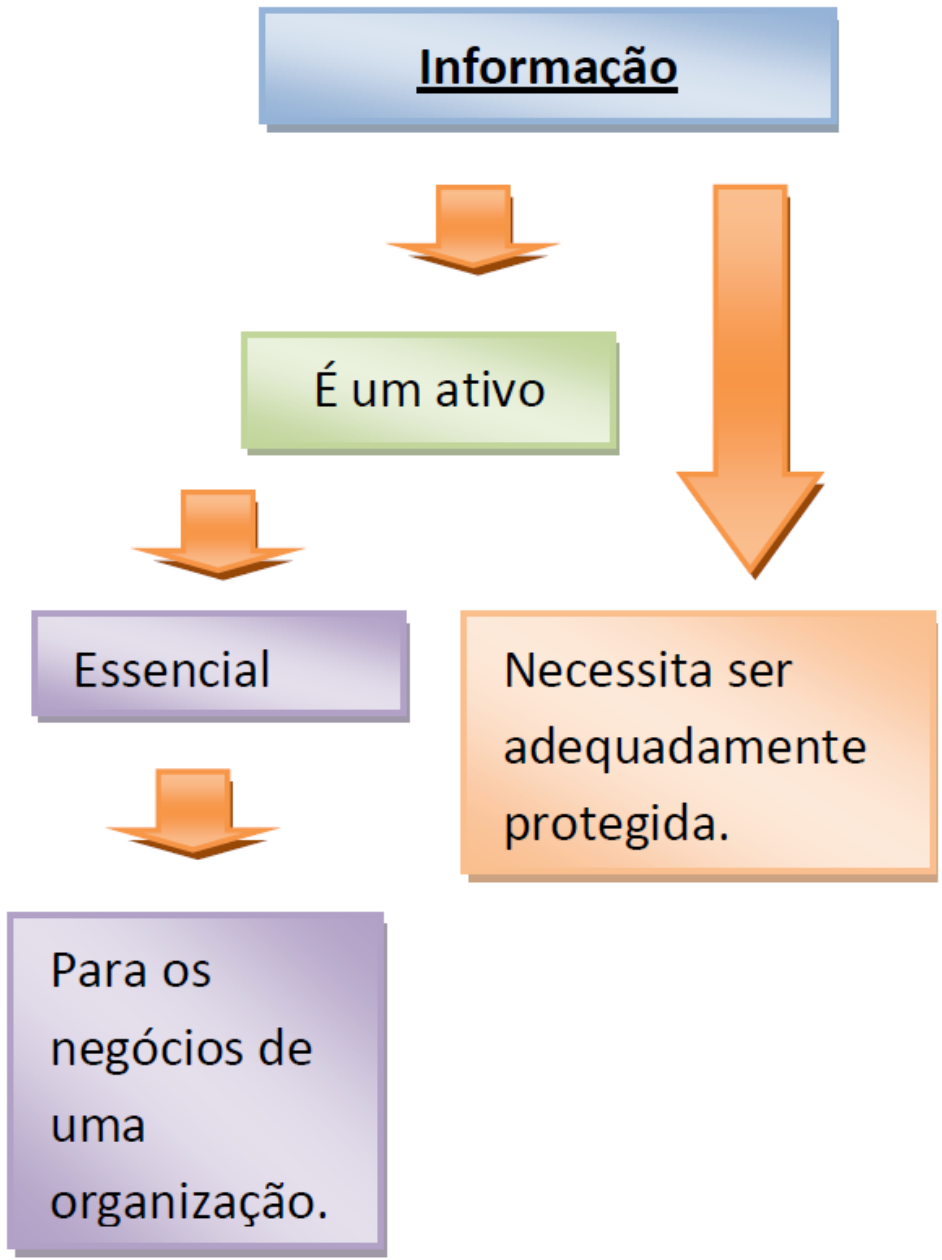
Práticas

Procedimentos

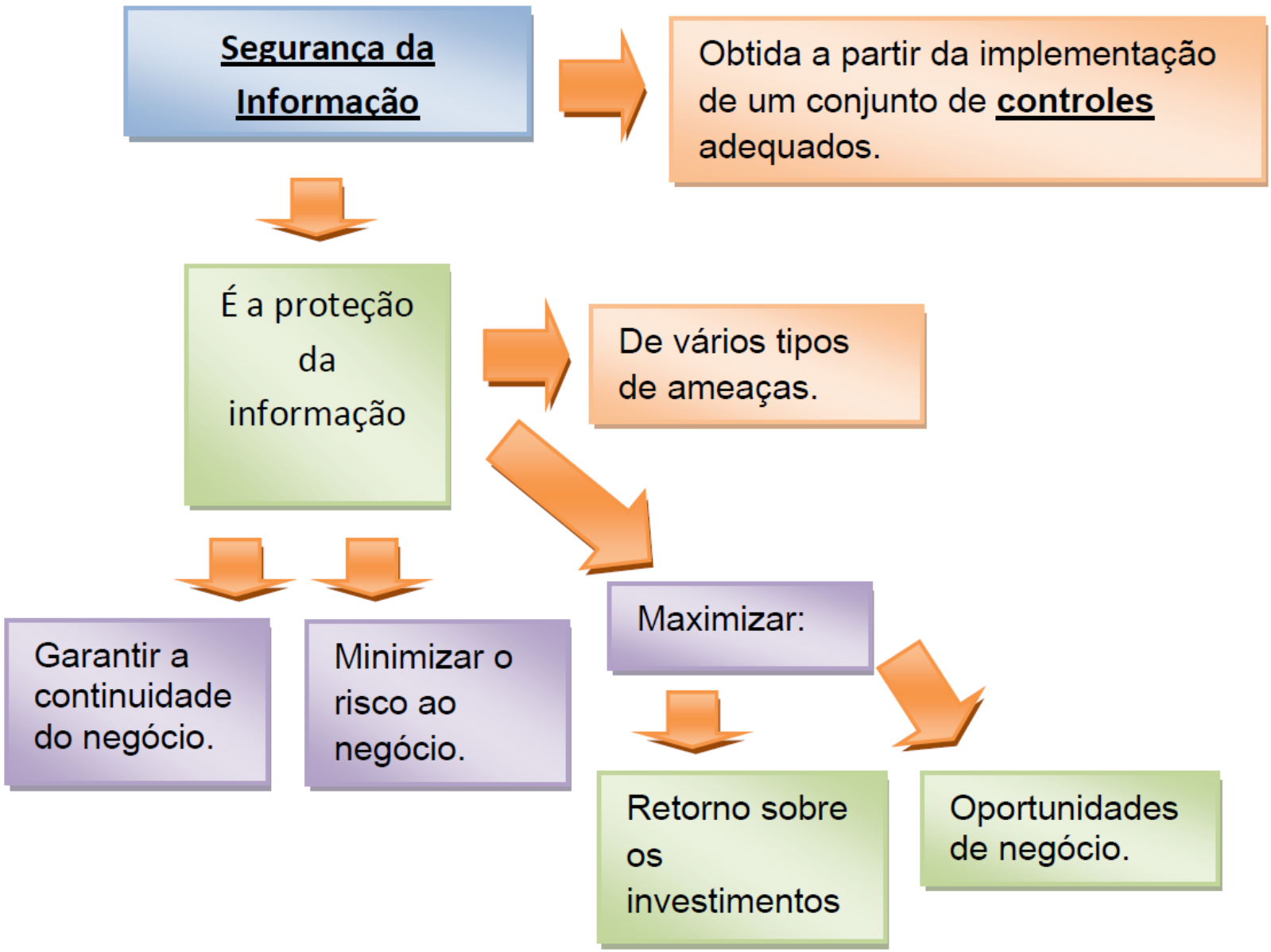
Estruturas organizacionais

Funções de softwares/hardware

Informação


Informação
É um ativo
Essencial
Para os negócios de uma organização.
Necessita ser adequadamente protegida.

Segurança da Informação



Por que SI é necessária?

- As informações são constantemente colocadas à prova por diversos tipos de ameaças
  - Fraudes eletrônicas, sabotagem, vandalismo, etc.
- Dependência nos sistemas de informação torna as organizações mais vulneráveis às ameaças
  - Controle de acesso é cada vez mais difícil
- Sistemas de informação não foram projetados para serem seguros
  - Codificação segura (evita buffer overflow, SQL Injection, PHP Injection, etc)

SI: Técnica X Gestão

- **A segurança que pode ser alcançada por meios técnicos é limitada**
- Deve ser apoiada por gestão e procedimentos
- Identificação dos controles a serem implantados requer planejamento cuidadoso e detalhado
- Todos funcionários devem participar, no mínimo
  - Talvez fornecedores, clientes, terceiros, etc.
- Consultoria pode ser necessária
- Controles são mais baratos e eficientes quando implantados em fases iniciais

Segurança Física

Segurança: Principais Ameaças

- **Falhas em equipamentos, SO e aplicativos**
- **Acesso físico não autorizado (infraestrutura predial)**
- **Perda de comunicação voz e dados**
- **Vandalismo, roubo, furto**
- **Fatores naturais**
  - **Incêndio, Inundação, Furacões, Desabamentos**
  - **Explosões, Raios, Terremotos**
- **Fatores humanos envolvidos**
  - **Negligência**
  - **Despreparo**
  - **Desinformação**

Segurança Física

Algumas Proteções & Soluções

Cofres anti-fogo

Poucas mídias

Grande volume de mídias

Servidores

Sala-cofre

- **Paredes modulares**
- **Painel de controle**
- **Porta dupla**
- **Piso elevado**
- **Blindagem para cabos**
- **Revestimento anti-fogo**

Segurança Física

Mecanismos de Autenticação

Dispositivos de Autenticação

- O grau de segurança empregado depende do valor da informação que protege

- Tokens → o que você tem
- Passwords → o que você sabe
- Smart Cards → o que você sabe + o que você tem
- Autenticação biométrica → baseada em características do usuário - você é a senha!

Biometria

- Impressão digital
- Retina/Íris do olho
- Características faciais
- Reconhecimento de voz
- Geometria e veias das mãos
- Padrão de escrita
- Poros da pele
- Análise de DNA
- Formato da orelha
- Composição química do odor corporal
- Emissões térmicas
- Geometria dos dedos
- Identificação da unha
- Maneira de andar

Ataques
& Incidentes

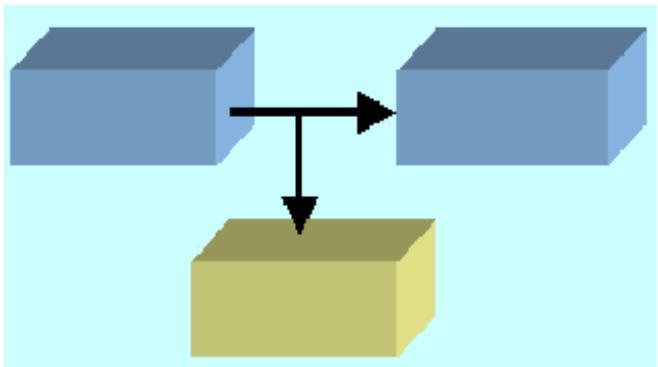
Tipos, Motivos, Efeitos

Morais da segurança

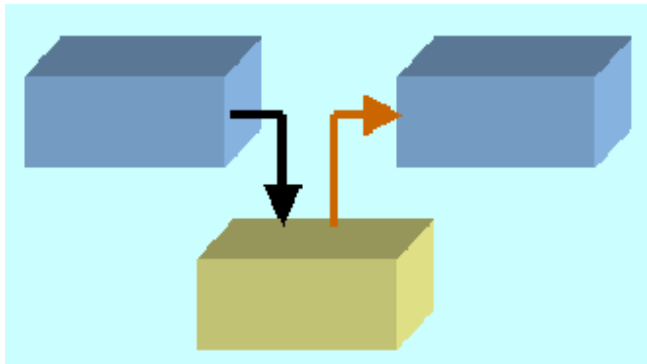
- As portas dos fundos são tão boas quanto as portas da frente.
- Uma corrente é tão forte quanto o seu elo mais fraco.
- Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.

Ataques

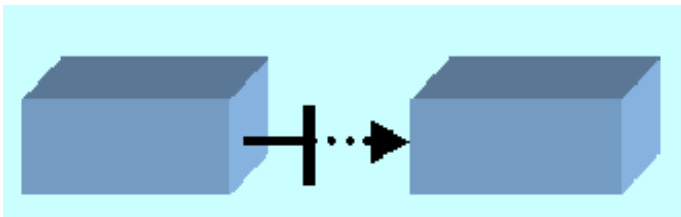
Interceptação



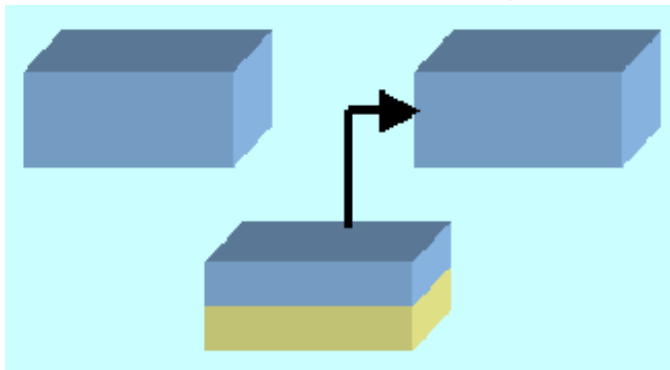
Modificação



Interrupção



Personificação



Ataques clássicos

- Kevin Mitnick
  - Preso de fevereiro de 1995 a janeiro de 2000
  - 25 acusações federais:
    - fraude no sistema telefônico, roubo de software proprietário (Sun, Motorola, Novell e Nokia)

Tipos de Ataques

- DoS - Negação de serviço
- Spam
- Phishing spam
- Ataques de força bruta
- Farejamento de pacotes (packet sniffing)
- Varreduras
- Ataques ao TCP/IP
- Malware
- Buraco negro, buraco cinza, On-Off, etc.
- outros

Malware (códigos maliciosos)

- Vírus
- Worms
- Bots
- Cavalos de Tróia
- Backdoors
- Keyloggers/Screenloggers
- Spywares
- Rootkits

Novos desafios para segurança

- Tecnologias sem fio
- Dispositivos móveis
- Internet das Coisas
- Cidades Inteligentes
- Redes sociais on-line
- Computação em nuvem

O que podemos utilizar para diminuir os riscos?

- Educação do usuário final
- Antivírus
- Antispyware
- Filtro AntiSpam
- Backup dos Dados
- Criptografia
- Firewall
- Sistemas de Detecção de Intrusão
- Blockchain
- Política de segurança
- Gestão de segurança da informação
- Outros.

Tendências da Segurança

- Era de ouro do hacking?
- Adoção rápida de novas técnicas e tecnologias, muitas delas não testadas
- Utilizamos algumas dessas tecnologias para a proteção da informação
- Grande número de vulnerabilidades
- Informações amplamente disponíveis para o aprendizado

Tendências – Cenário pessimista

- O expertise dos hackers está aumentando
- A sofisticação dos ataques e das ferramentas de ataque está aumentando
- A efetividade das invasões está aumentando
- O número de invasões está aumentando
- O número de usuários da Internet está aumentando
- A complexidade dos protocolos, das aplicações e da rede está aumentando
- A complexidade da própria Internet está aumentando
- Existem problemas de projeto na infraestrutura da informação
- O ciclo de desenvolvimento e testes de software está diminuindo
- Softwares com vulnerabilidades, algumas repetidas, continuam sendo desenvolvidos

Tendências – Cenário otimista

- Desenvolvimento de software com preocupação com a segurança
- Projetos de rede com preocupação com a segurança
- Segurança fazendo parte de qualquer aspecto da tecnologia, assim como a qualidade faz parte de produtos e processos