# Segurança de Redes

FUMEC
Upgrade Ciência da Computação
Márcio H. C. d'Ávila
2001 / 1º Semestre

## Sumário

- Introdução a Segurança
- Vulnerabilidades, Ameaças e Ataques
- Criptografia
- Autenticação
- Segurança de E-mail
- Segurança na Web
- Segurança de Rede
- Segurança de Sistema
- Redes Privadas Virtuais (VPN)
- Firewalls
- Planejamento de Segurança

# Referências

- **Web – Acompanhamento das aulas**
  http://www.inet.com.br/~mhavila/aulas/seguranca/

- **Bibliografia Principal**
  [1] Canavan, John E. **Fundamentals of Network Security**. Artech House, 2001, 380 pp. ISBN 1580531768

  [2] Stallings, William. **Network Security Essentials: Applications and Standards**. Prentice Hall, 1999, 366 pp. ISBN 0130160938



# Referências

- **Bibliografia Complementar**
  [3] Network Security: Private Communication in a Public World

  [4] Segurança.com - Segredos e Mentiras sobre a Proteção na Vida Digital

  [5] Segurança de Redes - Projeto e Gerenciamento de Redes Seguras

  [6] Hackers Expostos: Segredos e Soluções para a Segurança de Redes. (lançada 2ª edição EUA)

  [7] Segurança Máxima. Tradução da 2ª edição

  [8] Practical Unix and Internet Security. 2nd Edition

# Introdução

- Computadores são mais úteis ligados em rede, compartilhando informação e recursos
  - Disponibilização ampla de informação
  - Interoperabilidade e intercâmbio de informação
  - Mobilidade de acesso e gerenciamento remoto
  - Sistemas de processamento distribuído
- A partir dos anos 80: evolução das interconexões de redes de computadores
- Aumento de extensão das redes e do acesso: mais necessidade de cuidado e controle



# Introdução

- A todo momento surgem novos casos de redes invadidas ou comprometidas por ação de hackers, vírus e outros fatores de risco
- Estatísticas
  - Estudo do American Society for Industrial Security (ASIS) e Price Waterhouse-Cooper, EUA ,1999:
    - 97 empresas da lista Fortune 1000 responderam
    - Mais de US$45 bilhões em perda/roubo de informação
    - Média: 2,45 incidentes e US$0,5 milhão por incidente
    - Número de incidentes reportados por mês é crescente

# Introdução

- Estatísticas
  - Levantamento anual de 2001 do FBI e Computer Security Institute (CSI) nos EUA:
    - Respostas de 538 atuantes no campo de segurança
    - 85% detectaram brechas de segurança nos últimos 20 meses e 70% declararam ter sofrido algum tipo de ataque nos últimos 12 meses
    - Perdas $ mais sérias: roubos de informação proprietária
    - 70% citam conexão Internet como ponto freqüente de ataque (2000: 59%) e 31% citam os sistemas internos da empresa
    - 45% reportaram invasões de fontes externas (2000: 25%)
    - 55% reportaram invasões não-autorizadas por uma fonte interna à organização
    - 91% têm abuso do acesso à Internet por funcionários (2000: 79%)
    - 94% detectaram vírus de computador (2000: 85%)
    - 36% recorreram à Justiça pelas invasões (2000: 25%, 1996: 16%)

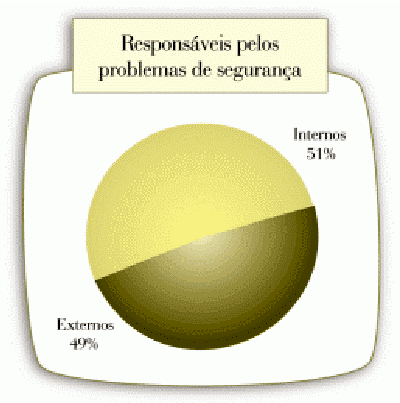


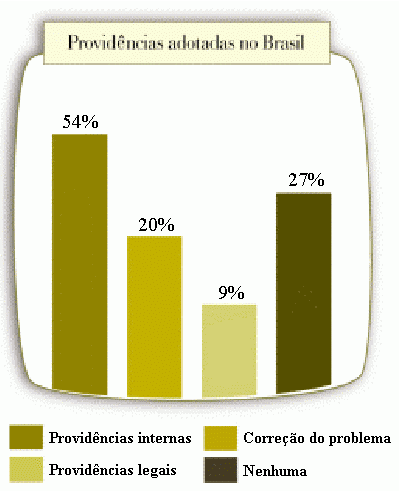
# Introdução

- Estatísticas
  - Brasil: Pesquisa Nacional sobre Segurança da Informação, Junho/2000:
    - 93% reconhecem importância da proteção de dados para o sucesso do negócio, 39% consideram vital para corporações
    - Controle das redes corporativas ainda é fraco: 41% não sabem se foram invadidas, 85% não sabem medir o prejuízo
    - 38% c/ acesso à Internet via modem, sem grande segurança
    - Vírus: maior ameaça (75%) e 48% de contaminação nos últimos 6 meses, mesmo 93% adotando meios de prevenção
    - Causa interna: funcionários 39%, HD defeito 6%, prestadores de serviço 6%. Causa externa: hackers 28%, clientes 7%, fornecedores 6%, estudantes 6%, concorrentes 2%

# Introdução

- Pesquisa Nacional (cont.)






# Segurança

- Importância da segurança de redes
  - Proteção de patrimônio (em especial: informação)
  - Credibilidade e vantagem competitiva
  - Cumprimento de responsabilidades
  - Continuidade de operação/atividade
- Segurança de redes
  - Segurança de computadores
  - Segurança da informação
- Segurança da informação =
  proteção + integridade + disponibilidade + autenticação

# Segurança

- Prática: Prevenção, Detecção e Resposta


- Toda segurança é relativa, pode ser tomada em níveis e deve ser um balanceamento:
  - custo da segurança × valor do patrimônio
  - provável × possível
  - necessidades de segurança × do negócio

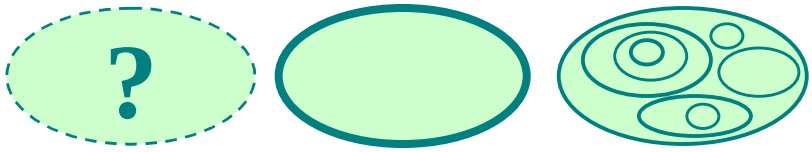


# Segurança

- Análise de risco
  - Identificar e priorizar valores (patrimônio)
  - Identificar vulnerabilidades
  - Identificar ameaças e suas probabilidades
  - Identificar contra-medidas (respostas)
  - Desenvolver análise de custo-benefício
  - Planejar políticas e procedimentos de segurança
- Políticas e procedimentos de segurança
  - Políticas: gerais, focam o que e porquê
  - Procedimentos: específicos e detalhados, focam quem, quando, como

# Segurança

- Modelos de segurança
  - Obscuridade
    - proteção pelo sigilo e desconhecimento
  - Defesa perimetral
    - proteção concentrada nos limites/bordas da rede
  - Defesa extensiva
    - cuidar da segurança de cada sistema componente






# Segurança

- Elementos e requisitos de segurança
  - **Identificação e Autenticação**: distinguir, determinar e validar a identidade do usuário/entidade (se é quem diz ser)
  - **Controle de acesso**: limitar/controlar nível de autorizações de usuários/entidades a uma rede, sistema ou informação
  - **Não-repúdio**: impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação
  - **Confidencialidade**: proteção da informação contra descoberta ou interceptação não autorizada; privacidade
  - **Integridade**: impedir informação/transmissão de ser altera-da/danificada de forma ñ-autorizada, imprevista ou acidental
  - **Disponibilidade**: confiabilidade de redes, sistemas e equipamentos sobre evitar ou se recuperar de interrupções