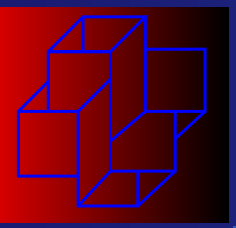
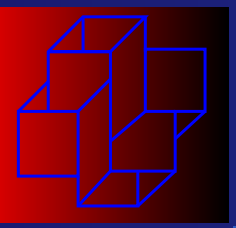


# Segurança da Informação

## *LNCC - FASE - Maio/2009*

Fábio Borges

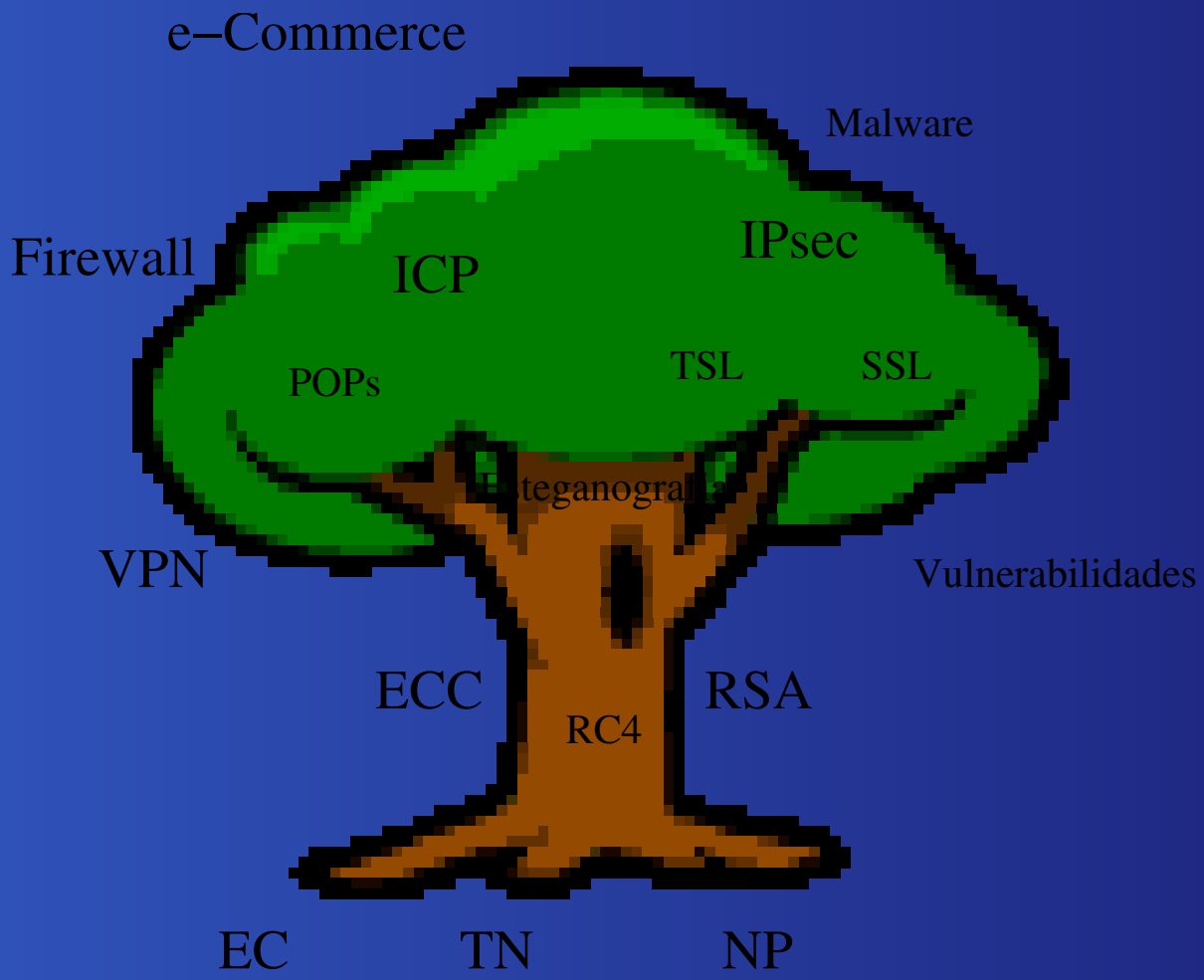


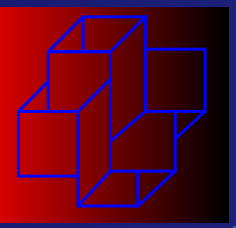
# Conhecimentos Necessários

- Redes de comunicação
- Sistemas computacionais
- Matemática
- Biologia (biometria)
- ADM (Metodologias e políticas)
- Eletrônica, Física, Lingüística...

# Missão Impossível

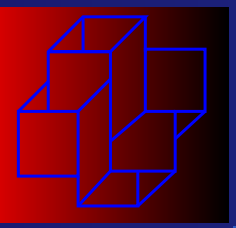
# Árvore da Segurança





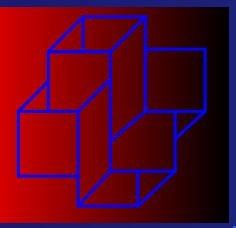
# Política de Segurança

- Política de uso aceitável



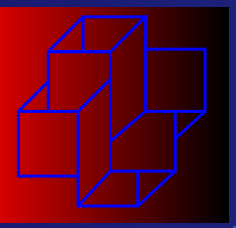
# Política de Segurança

- Política de uso aceitável
- Apoio político



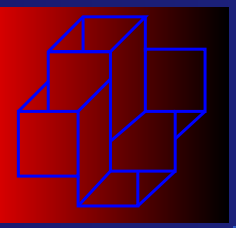
# Política de Segurança

- Política de uso aceitável
- Apoio político
- Definição de responsabilidades



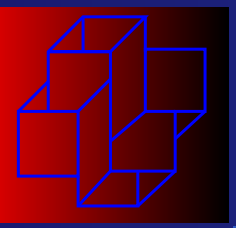
# Política de Segurança

- Política de uso aceitável
- Apoio político
- Definição de responsabilidades
- Deve ser implementada em software



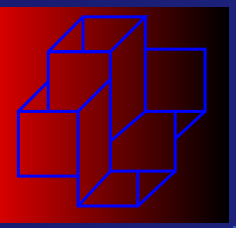
# Terminologia

- Mensagem - Plaintext



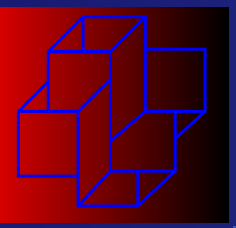
# Terminologia

- Mensagem - Plaintext
- Chave



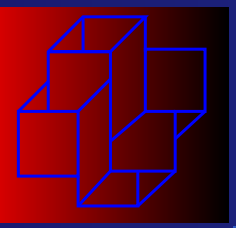
# Terminologia

- Mensagem - Plaintext
- Chave
- Criptograma - Ciphertext



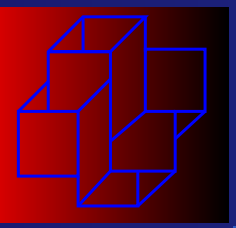
# Terminologia

- Mensagem - Plaintext
- Chave
- Criptograma - Ciphertext
- Criptossistema



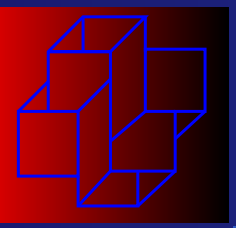
# Terminologia

- Mensagem - Plaintext
- Chave
- Criptograma - Ciphertext
- Criptossistema
- Criptografia



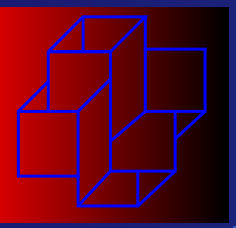
# Terminologia

- Mensagem - Plaintext
- Chave
- Criptograma - Ciphertext
- Criptossistema
- Criptografia
- Entropia



# Terminologia

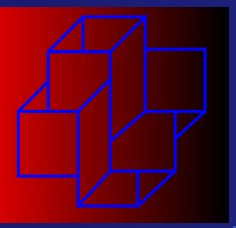
- Mensagem - Plaintext
- Chave
- Criptograma - Ciphertext
- Criptossistema
- Criptografia
- Entropia
- Esteganografia



# Esteganografia

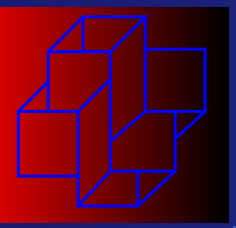
Original:

Esteganografia:



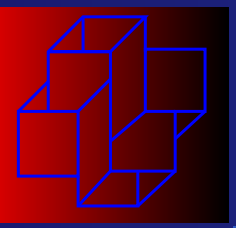
# Entropia

$$H(\xi) = -\sum_{C=\xi} P(\xi) \log_2 (P(\xi))$$



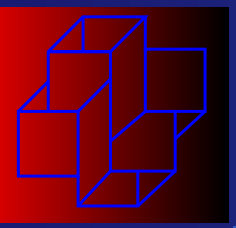
# Ataques Comuns

- Força bruta



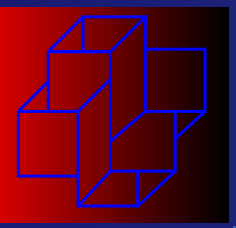
# Ataques Comuns

- Força bruta
- Soft Attacks



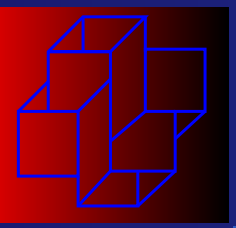
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise



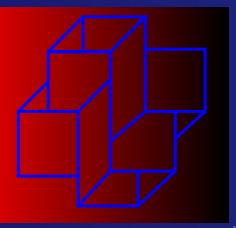
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)



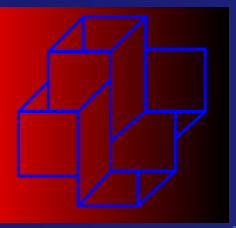
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle



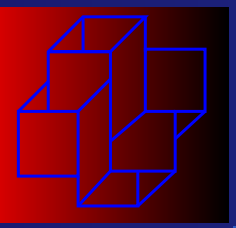
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware



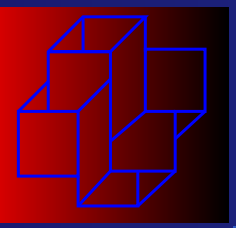
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing



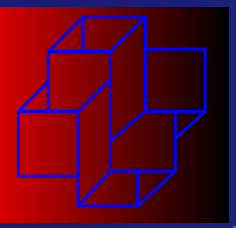
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing
- Defacement



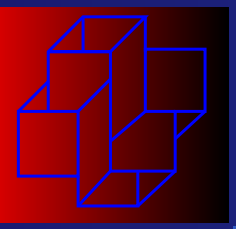
# Ataques Comuns

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing
- Defacement
- Phishing



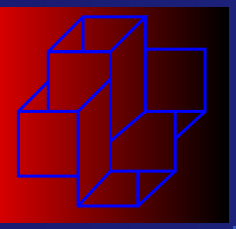
# Segurança em Pensamento

- Pense em um número inteiro de 1 a 9
- Multiplique seu valor por 9
- Some os dois algarismos deste produto!
- Some 7 ao resultado
- Divida o resultado por 4
- Faca a conversão do número por uma letra do alfabeto Ex.: $1 \rightarrow a, 2 \rightarrow b, 3 \rightarrow c \ldots$
- Pense em um país com esta letra
- Ache a $5^a$ letra deste país
- Pense em um animal com esta letra



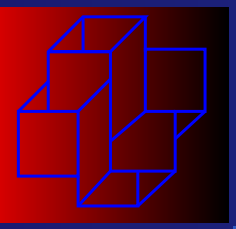
# Alguns Malware

- Keylogger



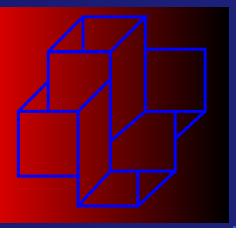
# Alguns Malware

- Keylogger
- Root-kit



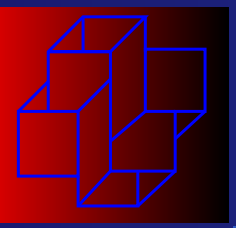
# Alguns Malware

- Keylogger
- Root-kit
- Spyware



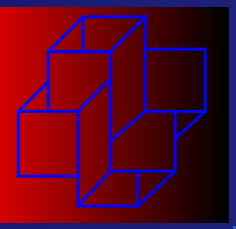
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware



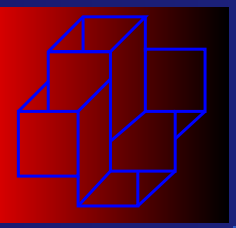
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus



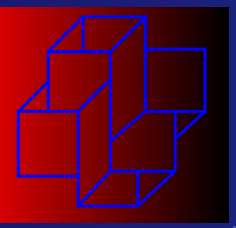
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms



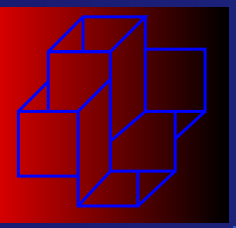
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)



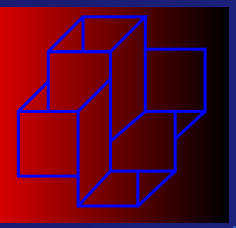
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)
- Backdoor (BackOrifice e NetBus)



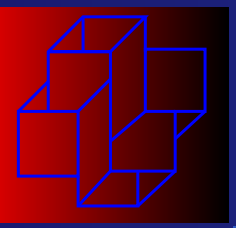
# Alguns Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)
- Backdoor (BackOrifice e NetBus)
- Hoax



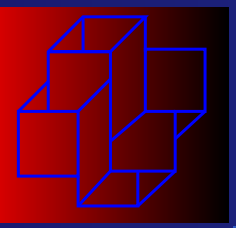
# Eliminar Protocolos sem Criptografia

- 23 - Telnet



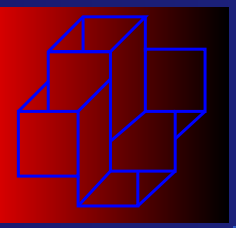
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP



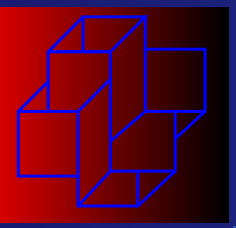
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3



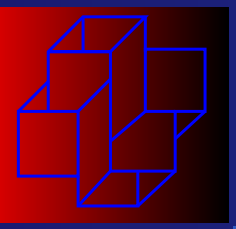
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP



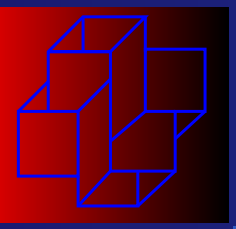
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin



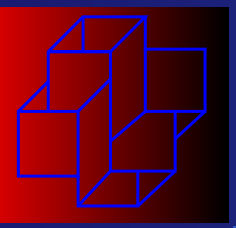
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh



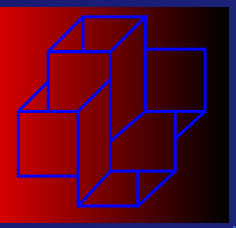
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec



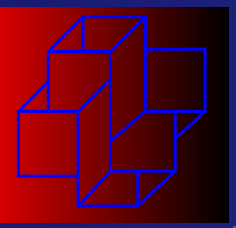
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec
- 6000 - X11 (com dados confidenciais)



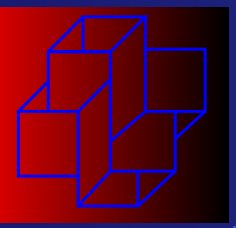
# Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec
- 6000 - X11 (com dados confidenciais)
- 80 - HTTP (com dados confidenciais)



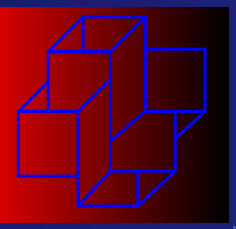
# Ferramentas Básicas

- nessus



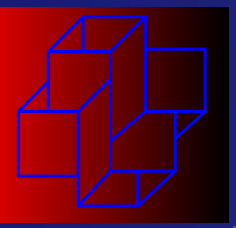
# Ferramentas Básicas

- nessus
- nmap



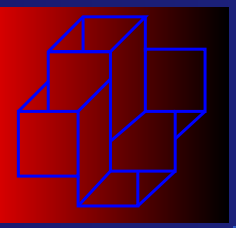
# Ferramentas Básicas

- nessus
- nmap
- lsof



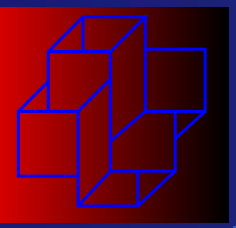
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal



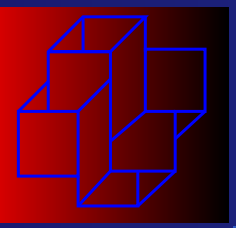
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump



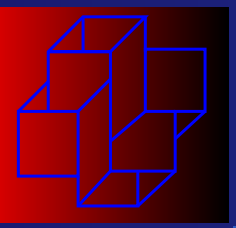
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top



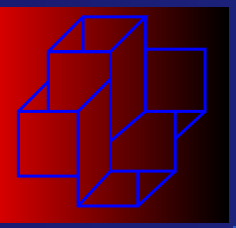
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois



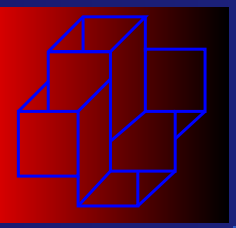
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute



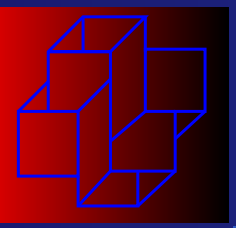
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute
- John the Ripper



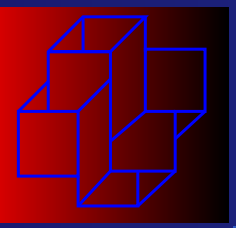
# Ferramentas Básicas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute
- John the Ripper
- firefox



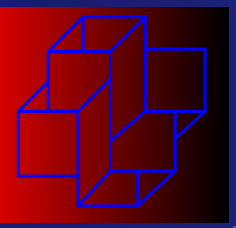
# Notícias

- Malware Wimad infecta arquivos de áudio
- HD à venda no eBay com dados sigilosos sobre mísseis dos EUA
- 12 milhões de novos PCs zumbis em 2009
- Piratas virtuais anunciam "sequestro"de dados e exigem US$ 10 milhões nos EUA
- Brasil é vice-campeão mundial de spam
- Empresas demoram para aplicar correções
- 42% das empresas gastarão mais com segurança



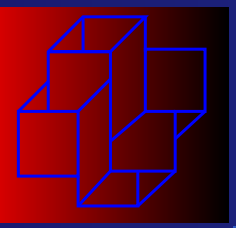
# Notícias

- 20% dos usuários não adota patchs do Windows
- Piratas virtuais atacam Departamento de Polícia de Nova York
- Descoberta a primeira rede de Macs zumbis
- Spam polui tanto quanto 3 milhões de carros
- Cracker invade Vírtua e muda DNS do Bradesco
- Mais da metade dos vírus no Brasil roubam dados



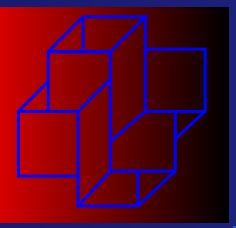
# Notícias

- Brasil é $5^o$ maior em atividade maliciosa
- Vírus Conflicker infecta parlamento inglês
- Canadá descobre maior rede de espionagem on-line da história
- Falha em chips Intel permite criar rootkits
- Criador da web foi vítima de fraude na internet
- Roubo de identidade cresce 800% em 6 meses
- Redes zumbi de celulares estão próximas



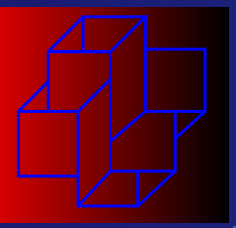
# Notícias

- Fraude na web causa rombo de R$ 500 mi ao ano
- SSL. Será que é seguro mesmo?
- Testes falsos dão nota 10 a falsos antivírus
- Invasão de hacker faz Citibank recolher cartões no Brasil
- Rede de computadores do governo federal registra 87 ataques virtuais por hora
- Novo vírus "mutante"infecta 2,5 milhões de PCs



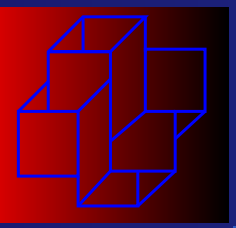
# Segurança na Rede

- o comércio eletrônico é seguro?



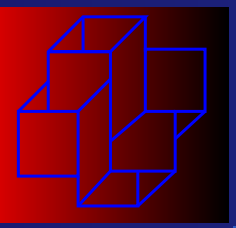
# Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?



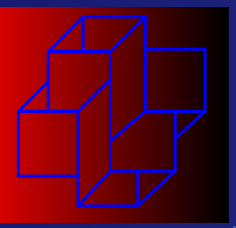
# Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?



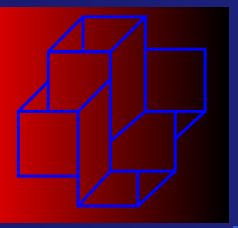
# Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?



# Segurança na Rede

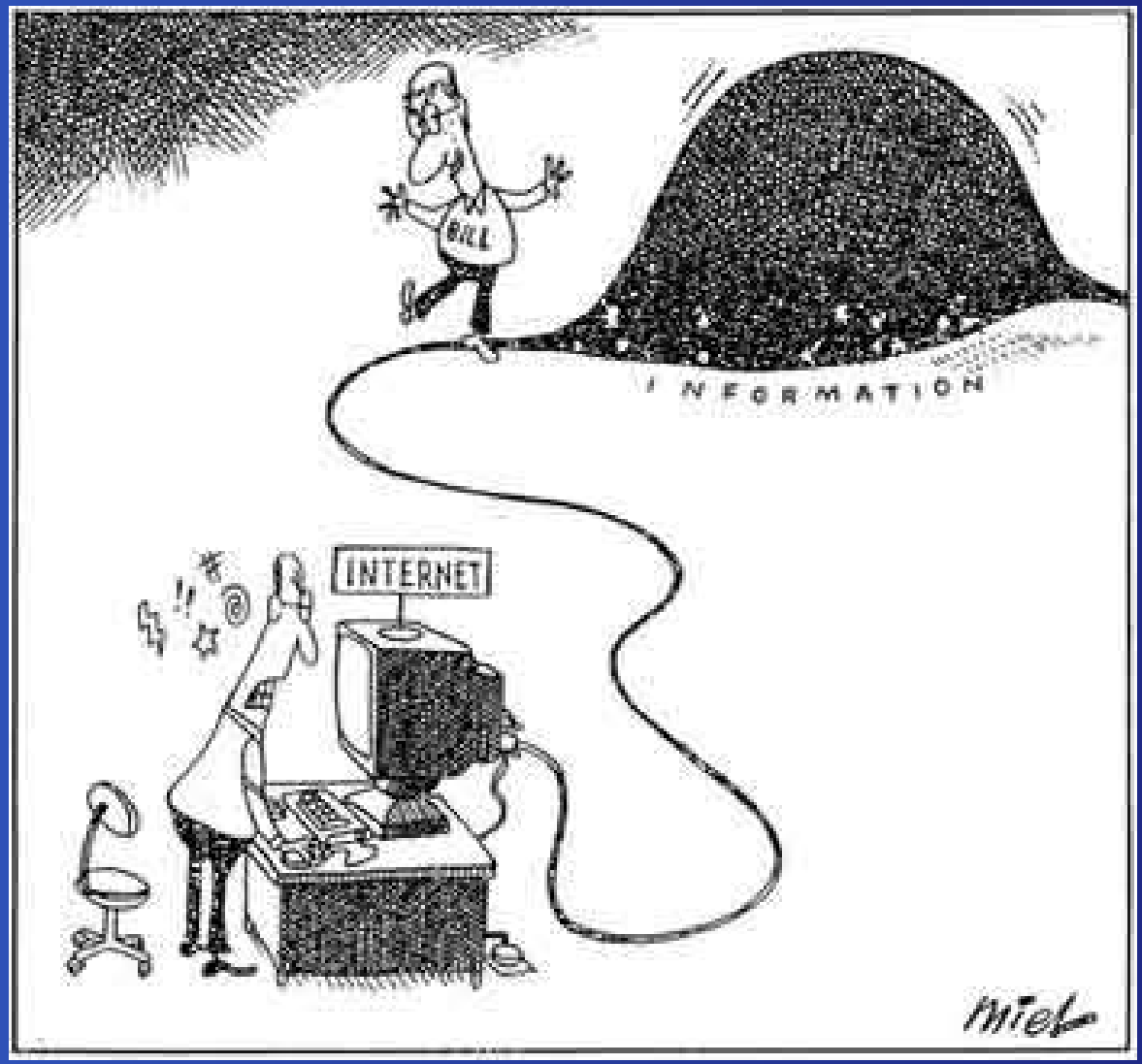
- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?
- onde está a segurança na rede?

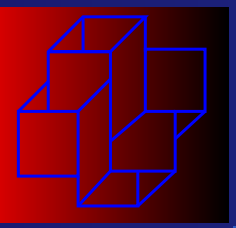


# Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?
- onde está a segurança na rede?
- onde está a insegurança na rede?

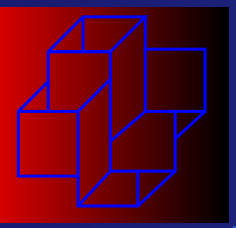
# Ameaça





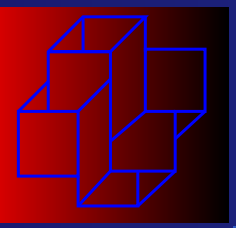
# Proteção na Rede

- ACL - Roteador



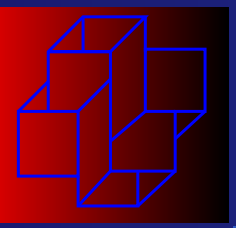
# Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)



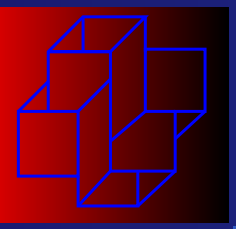
# Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall



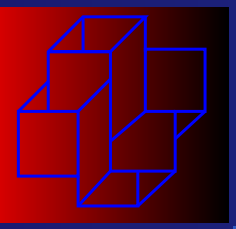
# Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS



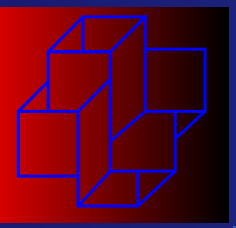
# Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS
- Honeypots e Honeynets



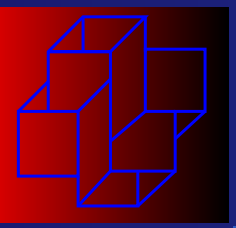
# Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS
- Honeypots e Honeynets
- Log-analyzer



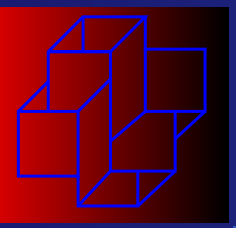
# Proteção Local

- Antispam (Junk mail controls)



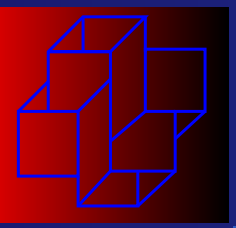
# Proteção Local

- Antispam (Junk mail controls)
- Antivírus



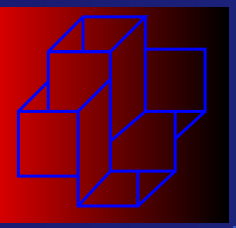
# Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy



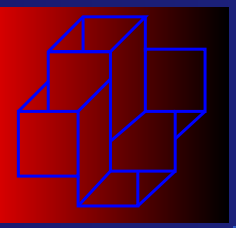
# Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal



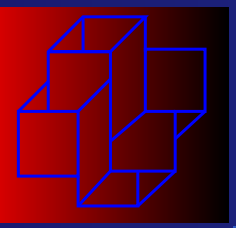
# Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal
- Anti-popup

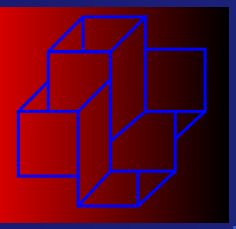


# Proteção Local

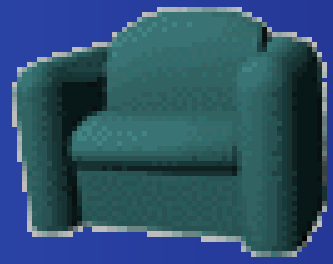
- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal
- Anti-popup
- Block loading of remote object in mail

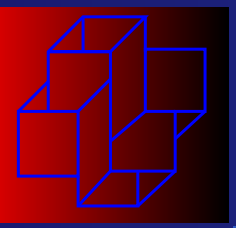


# Check-in



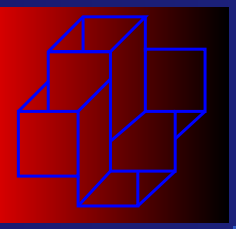
# Descansar?





# Atualização

"Segurança não é um produto, . . .
. . . mas um processo."



# Último Slide

- Obrigado!
- Quaisquer sugestões serão bem-vindas.