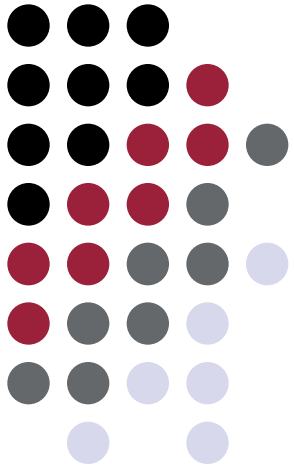
Segurança da Informação

CEA145 – Teoria e Fundamentos de Sistemas de Informação

Prof. MSc. George H. G. Fonseca
Universidade Federal de Ouro Preto



Introdução

- Um computador conectado à Internet sem firewall ou antivírus pode ser danificado em segundos
  - E se for um computador corporativo com dados confidenciais...

Introdução

- Acidentes e ataques também podem dizimar todos os dados de uma empresa desprevenida

Introdução

- Empresas precisam ter segurança e controle como prioridades
  - Segurança: procedimentos e medidas técnicas para garantir a confidencialidade, integridade e disponibilidade da informação

Vulnerabilidades e uso indevido dos SIs

- SIs são vulneráveis pois ao armazenar dados no formato eletrônico ficam expostos a mais tipos de ameaças

- Acesso não autorizado
- Erros

- Escuta clandestina *Sniffing*
- Roubo e fraude
- Alteração de mensagem

- Ciberpirataria
- Vírus e *worms*
- Vandalismo
- Ataque de recusa de serviço

- Roubo de dados
- Cópia / alt. de dados
- Falha de hardware/ SW

Software mal-intencionado

- Programas de software mal-intencionados são designados ***malware***
  - Vírus
  - Worms
  - Cavalo de tróia

Software mal-intencionado

- Vírus
  - Se anexa a outros programas ou dados a fim de serem executados sem a permissão do usuário
  - Quando executado, pode realizar diversos estragos: formatar o disco, entopir a memória, impedir a inicialização
  - São transmitidos na cópia de arquivos infectados

Software mal-intencionado

- *Worms*
  - Programas que se reproduzem automaticamente pela rede
  - São executados automaticamente e são tão devastadores quanto os vírus

Software mal-intencionado

- Cavalo de Troia
  - Software que parece benigno, mas depois faz algo diferente do esperado
  - Termo se refere ao cavalo de madeira usado pelos gregos para invadir Troia com guerreiros escondidos
  - Geralmente serve de porta de entrada para outros *malwares*

Software mal-intencionado

- SQL *injection*
  - Código SQL é inserido em formulários e para gerar comandos prejudiaicais ao Banco de Dados. Ex.:

    - USER: jo'; DROP TABLE clientes; --
    - PASS: 1234

    - Gera o seguinte comando no BD

```
SELECT user, pass
FROM clientes
WHERE user = 'jo'; DROP TABLE clientes ; --'
AND pass = '1234';
```

Software mal-intencionado

- *Spyware*
  - Programas que instalam-se no computador do usuário e monitora suas atividades a fim de usar as informações para *marketing*

- *Key loggers*
  - Categoria de *spyware* que registra as teclas pressionadas para detectar senhas de usuários

Hackers e Cibervandalismo

- *Hacker*
  - Indivíduo que pretende obter acesso não autorizado a um sistema de computador
  - O termo ***Cracker*** designa o *Hacker* com intenções criminosas (o *Hacker* pode, por exemplo, estar testando sistemas)

Hackers e Cibervandalismo

- Cibervandalismo
  - Interrupção, alteração da aparência de um site ou SI corporativo

Spoofing e Sniffing

- *Spoofing ou Phishing*
  - Disfarce de identidade que Hackers, por exemplo, e-mail falso
  - Envolve também o redirecionamento a sites falsos

Assunto: Policia Federal - Urgente
De: crimesdigitais@dpf.com.br
Data: 24-06-2006 04:13
Para:

Departamento de Polícia Federal

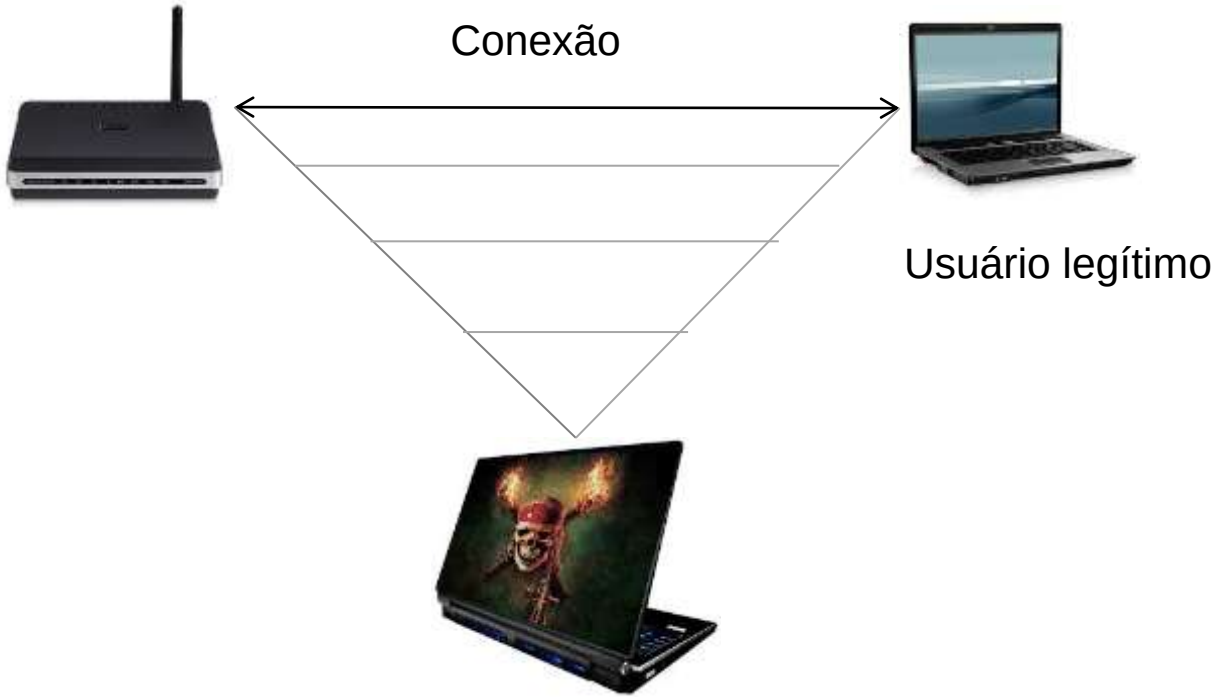
Senhor/Senhora,

Você teve sua máquina logada em um site ilegal.
Precisamos que esclareça o fato o mais rápido possível, caso não seja esclarecido em 24 horas, um inquérito será aberto.
Para entrar em contato com o Departamento da Polícia Federal e esclarecer o acontecimento clique aqui!

Superintendente:
DPF Daniel Gomes Sampaio
Endereço:
SAIS Quadra 7 - Lote 23 - Setor Policial Sul Brasília

Spoofing e *Sniffing*

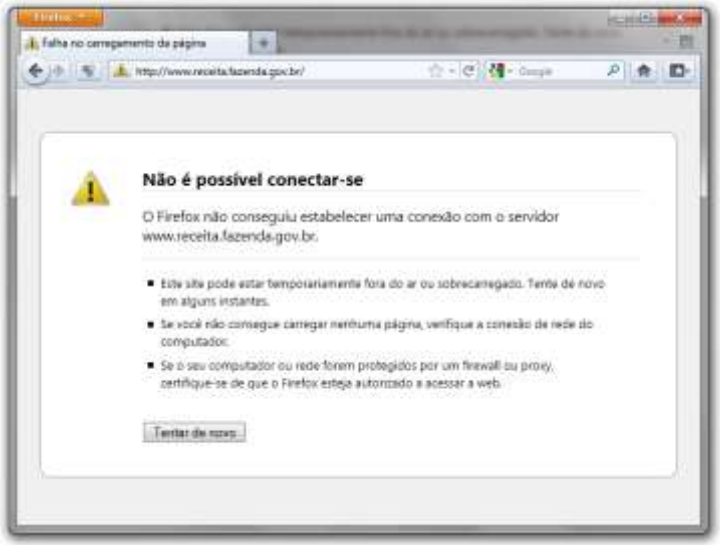
- *Sniffing*
  - Programa que monitora informações transmitidas pela rede



Ataques de Recusa de Serviço

- DoS (*Denial of Service*)
  - Hackers lotam um servidor com centenas de requisições falsas a fim de inutilizar a rede
  - A rede recebe tantas consultas que não consegue lidar com elas e ficam indisponíveis para solicitações de serviço legítimas
    - Exs.: Wikileaks em 2010

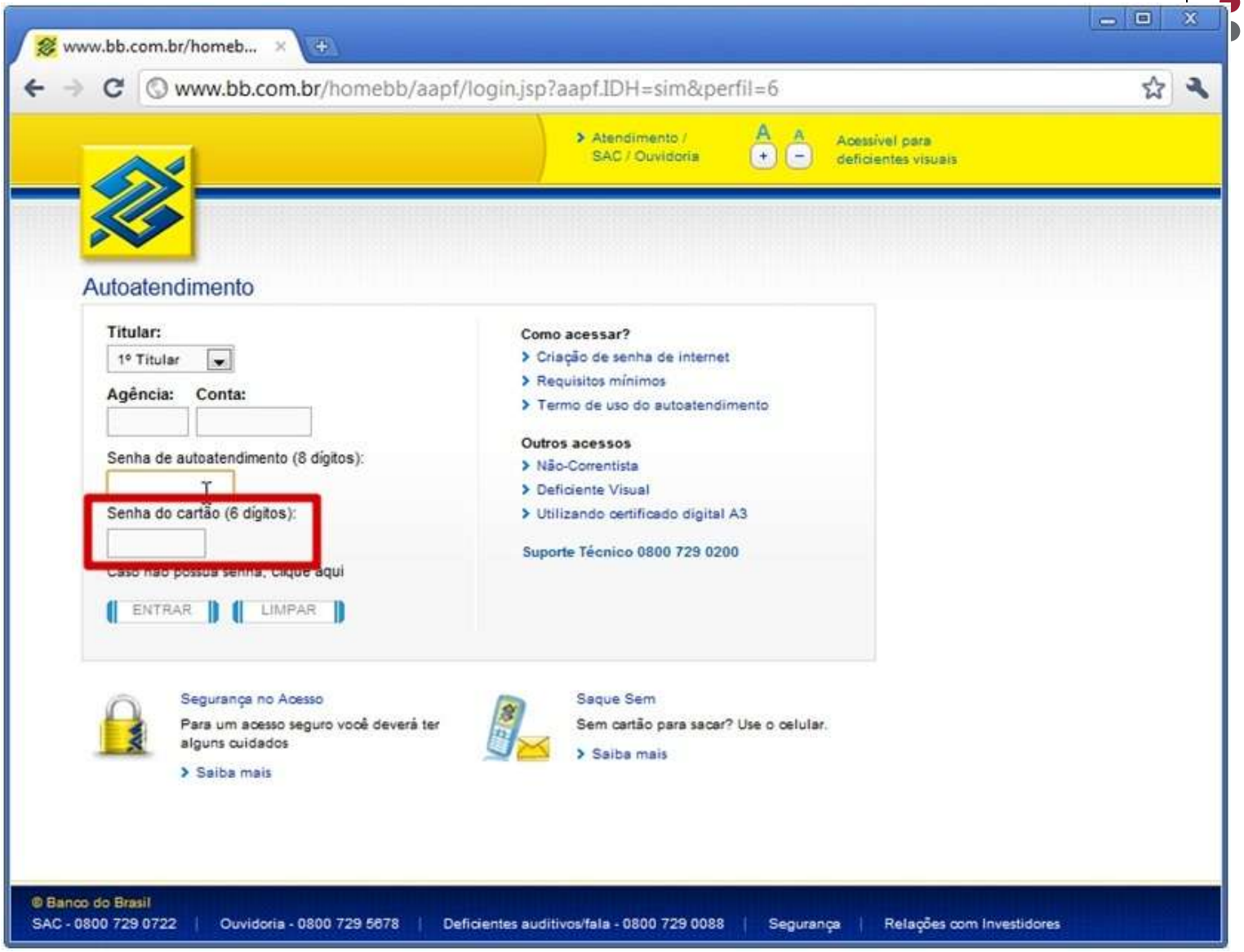
      Receita Federal em 2011



Roubo de Identidade

- Crime onde impostor obtém informações pessoais importantes como senha do cartão de crédito e CPF e se passa por outra pessoa
  - *E-commerce* facilita essa prática

Roubo de Identidade



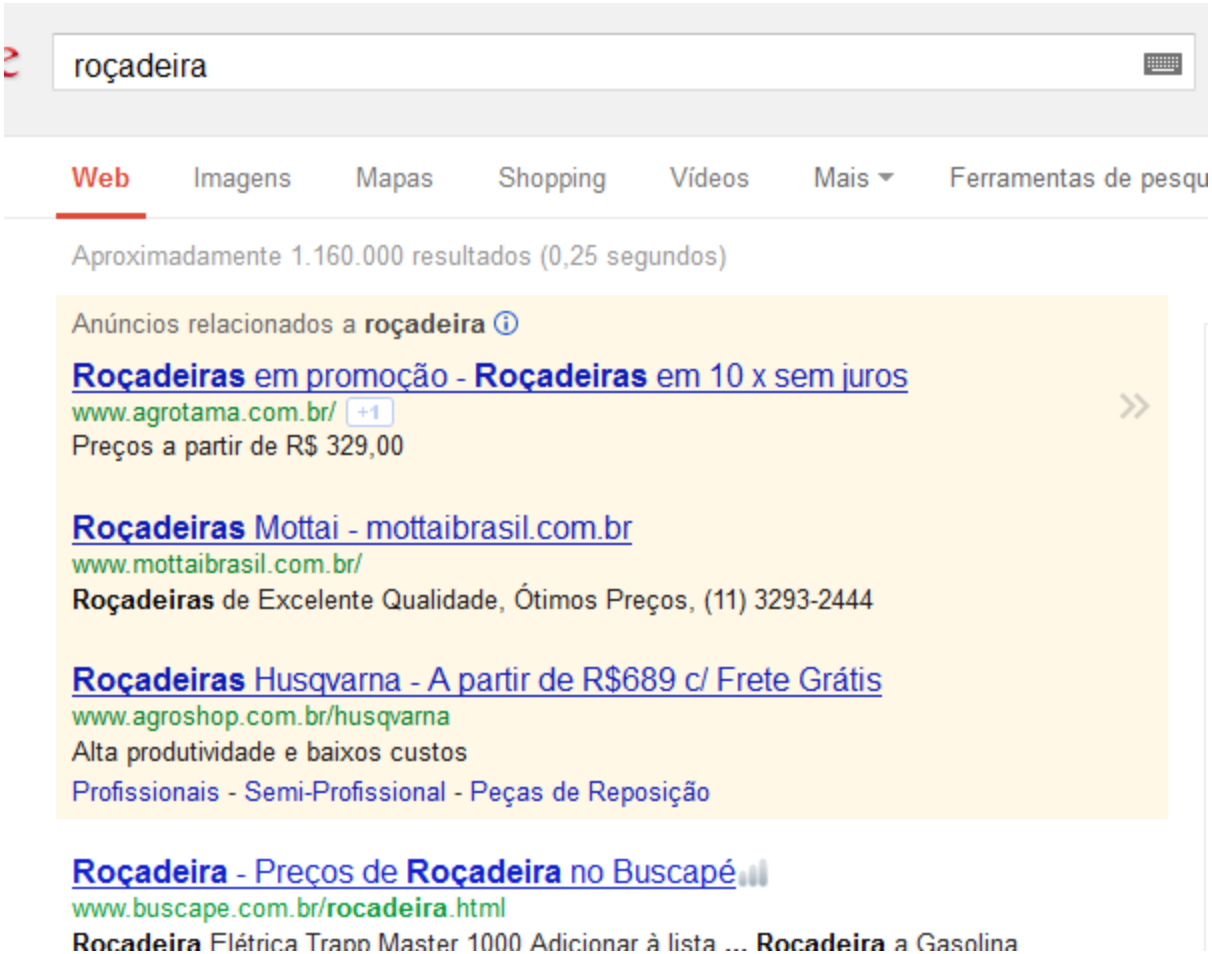
Roubo de Identidade

- *Evil twins*
  - Redes sem fio monitoradas por *hackers* que fingem oferecer conexão gratuita à Internet

Fraude do Clique

- Algumas propagandas são cobradas por cliques
- Indivíduo ou programa clica repetidamente em anúncio sem interesse no mesmo
- Empresas contratam pessoas para clicar em anúncios e aumentar os custos da concorrente com *marketing*

Fraude do Clique



Valor Empresarial da Segurança e do Controle

- Como a segurança não está diretamente relacionada à receita de vendas, muitas organizações relutam em gastar muito em segurança
  - No entanto, organizações têm ativos de informação valiosos
    - Registros médicos
    - Segredos de negócio
    - Informações sobre estratégias militares
  - Controle e segurança inadequados podem criar sérios riscos legais
    - Violação de privacidade
    - Corrupção de dados

Valor Empresarial da Segurança e do Controle

- Quanto investimento deve ser dedicado à Segurança da Informação?
- Avaliação de risco
  - Determina o nível de risco para a empresa caso uma atividade ou processo específico não sejam controlados adequadamente
  - Deve-se investir anualmente no máximo até o prejuízo esperado

Exposição	**Probabilidade de ocorrência (%)**	**Faixa de prejuízo / média ($)**	**Prejuízo anual esperado ($)**
Falta de energia elétrica	30	5.000-200.000 (102.500)	30.750
Ataque de negação de serviço	5	1.000-50.000 (25.500)	1.275
Erro de usuário	98	200-40.000 (20.100)	19.698

Valor Empresarial da Segurança e do Controle

- Prova eletrônica e Forense Computacional
  - Cada vez mais provas são apresentadas na forma de dados, como e-mails e transações de *e-commerce* pela Internet
  - Procedimento de coleta, exame, autenticação preservação e análise de dados mantidos em meios de armazenamento digital de maneira que possam ser usadas como prova em juízo
    - Recuperar dados sem prejudicar seu valor probatório
    - Armazenar e administrar com segurança os dados eletrônicos recuperados
    - Encontrar informações significativas em uma grande base de dados

Tecnologias e Ferramentas para a Segurança da Informação

- Controle de Acesso
  - Conjunto de políticas e procedimentos que uma empresa usa para evitar acesso indevido a seus sistemas por **pessoas não autorizadas dentro e fora da organização**

- O controle é feito pela **autenticação**

  - Capacidade de saber que uma pessoa é quem declara ser
  - Geralmente feita por meio de senha secreta
    - Senhas fáceis comprometem a segurança
  - Autenticação biométrica

Tecnologias e Ferramentas para a Segurança da Informação

- Firewall
  - Combinação de hardware e software que controla o fluxo de trafego que entra ou sai da rede
  - Age como um porteiro que verifica as credenciais de cada conexão
  - Usa regras de acesso
    - Ex.:

      Se IPcliente = “200.243.100.002”,

      recusar conexão;

      Se Requisição = “FTP”,

      recusar conexão;

Tecnologias e Ferramentas para a Segurança da Informação

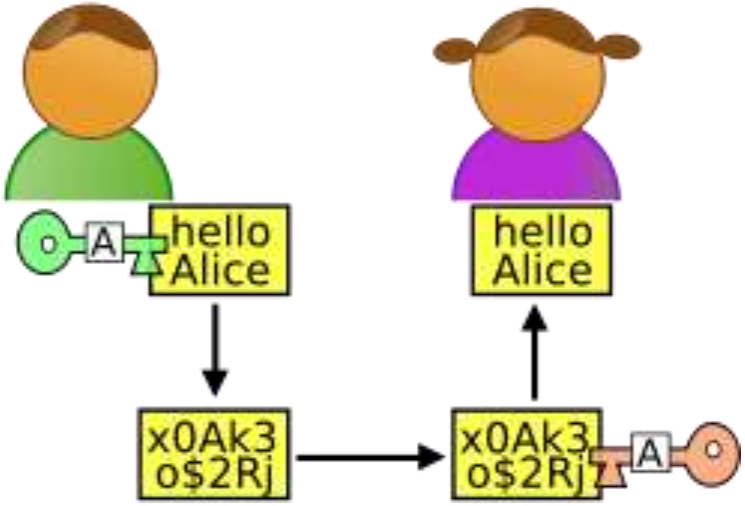
- Sistemas de Detecção de Invasão
  - Ferramentas de monitoração contínua instaladas nos pontos mais vulneráveis das redes coorporativas
  - Emite um alarme quando encontra um evento suspeito ou anômalo

Tecnologias e Ferramentas para a Segurança da Informação

- Software antivírus
  - Software projetado para verificar sistemas e processos a fim de detectar a presença de *malware* e eliminá-los

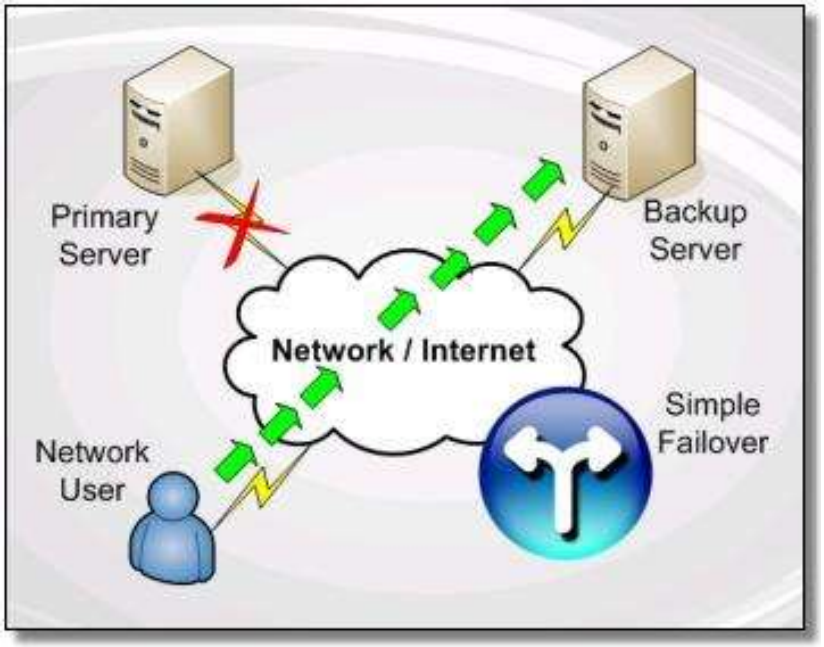
Tecnologias e Ferramentas para a Segurança da Informação

- Criptografia
  - Processo de transformar textos comuns ou dados em texto cifrado, legível somente ao destinatário



Tecnologias e Ferramentas para a Segurança da Informação

- Backups e redundância de hardware
  - Manter cópias de dados importantes da organização em outra(s) localidade(s) física(s) de modo a permitir sua recuperação em caso de sinistro



Aspectos Humanos da Segurança da Informação

- Apesar de algumas tecnologias colaborarem para a segurança da informação, o usuário continua sendo um elemento chave
  - Engenharia Social
    - Hackers se passam por outras pessoas para conquistar informações dos usuários
  - Os usuários devem ter conhecimento sobre algumas práticas de hackers e pessoas mal-intencionadas na Internet
    - Treinamento
  - Um usuário com conhecimentos sobre ameaças virtuais estará muito mais protegido

Aspectos Humanos da Segurança da Informação

- Um caso recente
  - Professora perde R$ 10 mil em golpe da página clonada do Banco do Brasil
  - http://g1.globo.com/al/alagoas/noticia/2013/03/professora-perde-r-10-mil-em-golpe-da-pagina-clonada-do-banco-do-brasil.html

Exercícios

- Por que as empresas devem garantir a segurança de seus sistemas de informação?
- Descreva algumas das ameaças às quais SIs estão expostos.
- Como se estabelece o valor a ser investido em Segurança da Informação?
- Descreva as principais tecnologias e ferramentas para salvaguardar recursos de informação.

Bibliografia

- *Sistemas de Informação Gerenciais*. Laudon, C. K.; Laudon, P. J.. 9a Edição, 2011.

- *Administração de Sistemas de Informação: Uma Introdução*. O'Brien, J. A.; Marakas, G. M. 13a Edição. São Paulo: McGraw-Hill, 2007.

- Artigos diversos

SBSI 2012
Cidades Inteligentes