

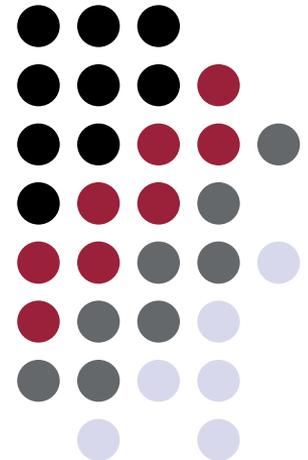
Segurança da Informação

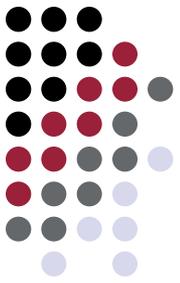


Universidade Federal
de Ouro Preto

CEA145 – Teoria e Fundamentos de Sistemas de Informação

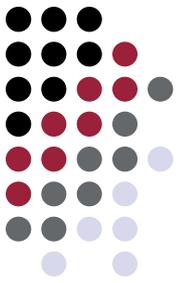
Prof. MSc. George H. G. Fonseca
Universidade Federal de Ouro Preto





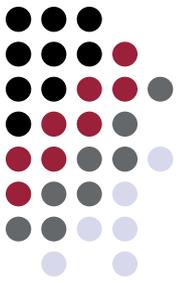
- Um computador conectado à Internet sem firewall ou antivírus pode ser danificado em segundos
 - E se for um computador corporativo com dados confidenciais...





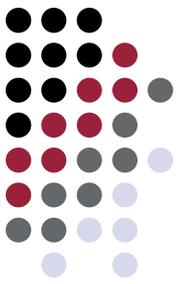
- Acidentes e ataques também podem dizimar todos os dados de uma empresa desprevenida





- 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

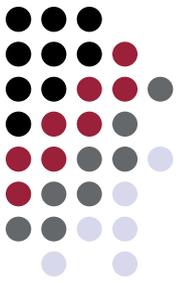


- SIs são vulneráveis pois ao armazenar dados no formato eletrônico ficam expostos a mais tipos de ameaças



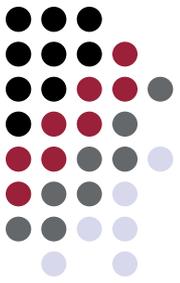
- Acesso não autorizado
- Erros
- Escuta clandestina *Sniffing*
- Roubo e fraude
- Alteração de mensagem
- Ciberpirataria
- Vírus e *worms*
- Vandalismo
- Ataque de recusa de serviço
- Roubo de dados
- Cópia / alt. de dados
- Falha de hardware/ SW

Software mal-intencionado



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

Software mal-intencionado

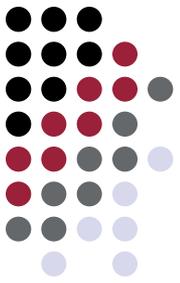


- Vírus

- 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

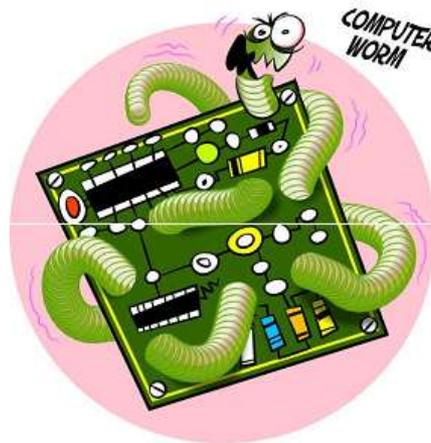


Software mal-intencionado

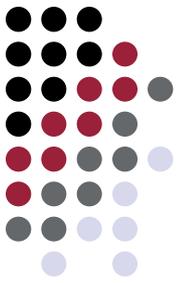


- *Worms*

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



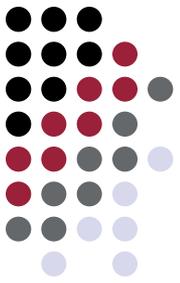
Software mal-intencionado



- 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 prejudiciais ao Banco de Dados. Ex.:

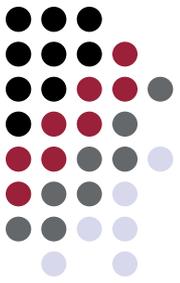
- USER: **jo'; DROP TABLE clientes; --**
- PASS: **1234**

- Gera o seguinte comando no BD

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



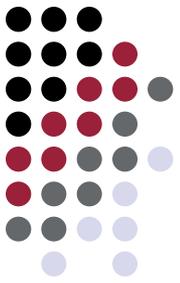
Software mal-intencionado



- *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

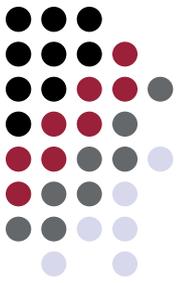


- *Hacker*

- 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

Martes 1 de junio de 2014 | Actualizado hace 7 minutos | Plan y plaza Bogotá | 1 4 3 6 | WTIEMPO | Ingreso | Registro

EL TIEMPO.COM | Buscar Noticias de Colombia y el Mundo

inicio | debes saber | debes hacer | debes leer | secciones | clasificados | archivo | ayudas

Te mas del día | Accidentes de tránsito | Grupo Ilu | Casa musical de la contratación en Bogotá | Lady Gaga | Música | Ja pin | Seguimos en: [Twitter] [Facebook]

Últimas Noticias

- 12:47 p.m. Dos desaparecidos por avalancha en zona rural de Toribío (Cauca)
- 12:25 p.m. Hospitalizados tres universitarios atropellados en el norte de Bogotá

Ver más últimas noticias | PATROCINADO PBL

Noticias de tu interés

- 12:31 p.m. Viernes, a más tardar, Gobierno decidirá extradición de Walid Makled
- 09:26 a.m. Ejército sirio se tomó la ciudad costera de Baniyas
- 01:10 a.m.

Ataque a web del Mininterior: ¿'Ciberactivismo' o 'Cibervandalismo'?

Por: REDACCIÓN EL TIEMPO.COM | 10:10 p.m. | 11 de Abril del 2011

Imagen de Anonymous_co, organización responsable del ciberataque. Foto: Twitter.zam

Comparte este artículo | [Facebook] Compartir | [Twitter] 20 | [LinkedIn] 3

Recomendar | 383 personas recomiendan esto. Sé el primero de tus amigos.

Ocho horas estuvo caída la página web del Ministerio del Interior en protesta a la Ley Lleras.

Recomendaciones

- Ataque a web de Ministerio del Interior
- Medio Libre, Bravo Pérez y 381 personas compartieron esto.

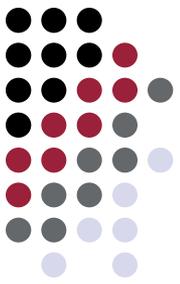
[Más en social de Facebook]

Top de noticias

Leído | Compartido

- 1 A lo cibernético: ciberataque causó tragedia en estado de emergencia
- 2 Lady Gaga sufrió aparatoso caída durante una presentación
- 3 La Prisión de la famosa Toño de Gabo y el grupo de Barranquilla
- 4 Los Nube tienen una maleta de pruebas para prender

Spooftng e Sniffing

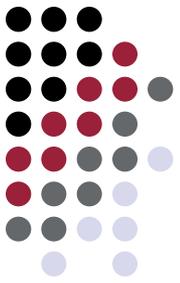


- *Spooftng ou Phishing*

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

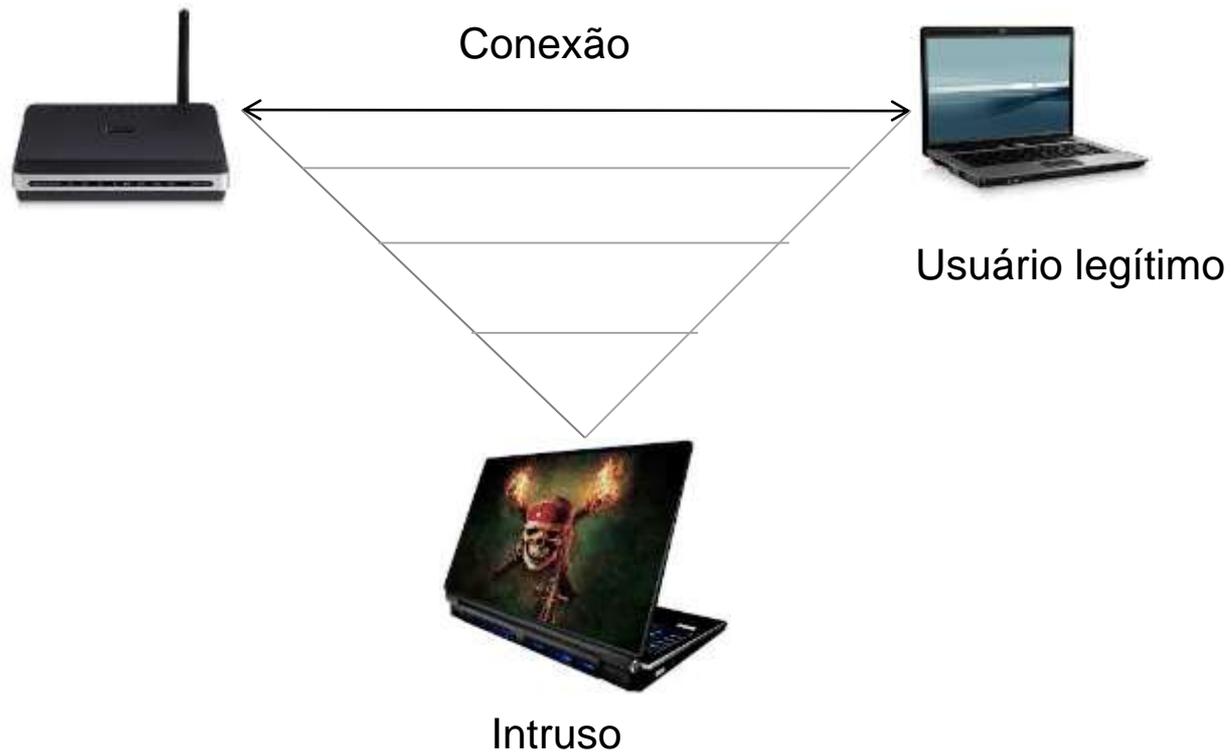


Spoofting e Sniffing

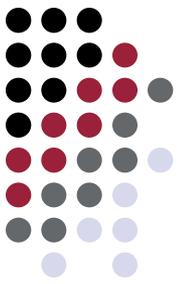


- *Sniffing*

- Programa que monitora informações transmitidas pela rede



Ataques de Recusa de Serviço

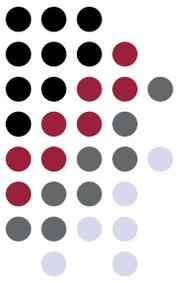


- **DoS (*Denial of Service*)**

- 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

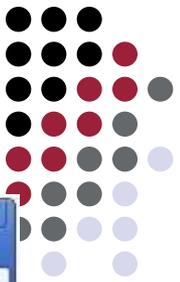


Roubo de Identidade



- 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



www.bb.com.br/homeb... x

www.bb.com.br/homebb/aapf/login.jsp?aapf.IDH=sim&perfil=6

Atendimento / SAC / Ouvidoria

Acessível para deficientes visuais



Autoatendimento

Titular:
1º Titular

Agência: **Conta:**

Senha de autoatendimento (8 dígitos):

Senha do cartão (6 dígitos):

Caso não possua senha, clique aqui

ENTRAR LIMPAR

Como acessar?

- > Criação de senha de internet
- > Requisitos mínimos
- > Termo de uso do autoatendimento

Outros acessos

- > Não-Correntista
- > Deficiente Visual
- > Utilizando certificado digital A3

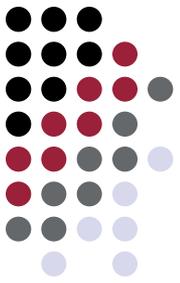
Suporte Técnico 0800 729 0200

Segurança no Acesso
Para um acesso seguro você deverá ter alguns cuidados
> Saiba mais

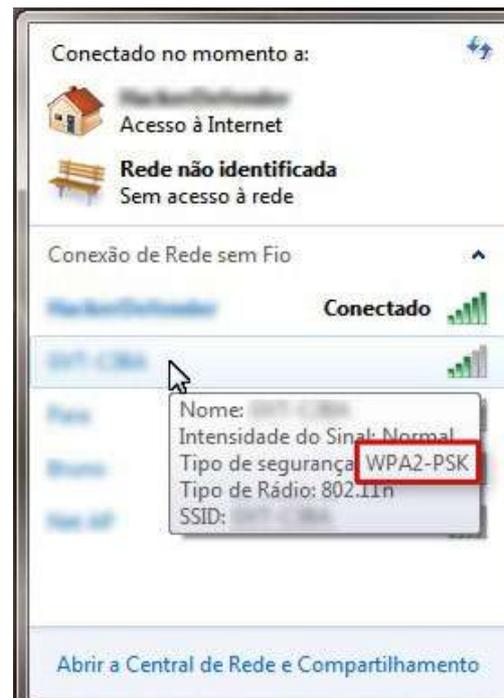
Saque Sem
Sem cartão para sacar? Use o celular.
> Saiba mais

© Banco do Brasil
SAC - 0800 729 0722 | Ouvidoria - 0800 729 5678 | Deficientes auditivos/fala - 0800 729 0088 | Segurança | Relações com Investidores

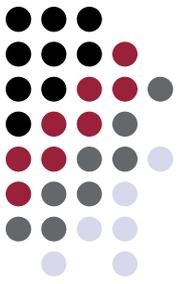
Roubo de Identidade



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

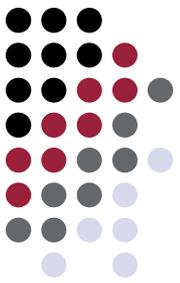


Fraude do Clique



- 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



roçadeira

Web Imagens Mapas Shopping Vídeos Mais ▾ Ferramentas de pesqu

Aproximadamente 1.160.000 resultados (0,25 segundos)

Anúncios relacionados a **roçadeira** ⓘ

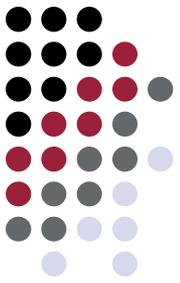
Roçadeiras em promoção - Roçadeiras em 10 x sem juros >>
www.agrotama.com.br/ +1
Preços a partir de R\$ 329,00

Roçadeiras Mottai - mottaibrasil.com.br
www.mottaibrasil.com.br/
Roçadeiras de Excelente Qualidade, Ótimos Preços, (11) 3293-2444

Roçadeiras Husqvarna - A partir de R\$689 c/ Frete Grátis
www.agroshop.com.br/husqvarna
Alta produtividade e baixos custos
Profissionais - Semi-Profissional - Peças de Reposição

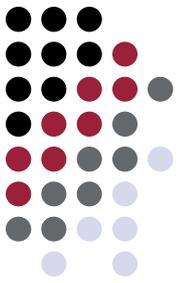
Roçadeira - Preços de Roçadeira no Buscapé 📶
www.buscape.com.br/rocadeira.html
Roçadeira Flétrica Trapp Master 1000 Adicionar à lista ... Roçadeira a Gasolina

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

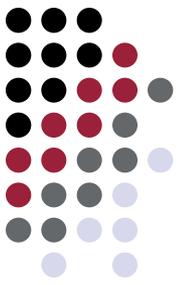
Valor Empresarial da Segurança e do Controle



- 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

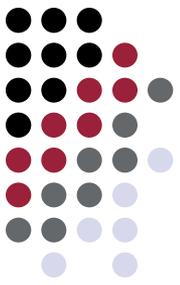
Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo / média (\$)	Prejuízo anual esperado (\$)
Falta de energia elétrica	30	5.000-200.000 (102.500)	30.750
Ataque de negação de serviço	5	1.000-50.000 (25.500)	1.275
Erro de usuário	98	200-40.000 (20.100)	19.698

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

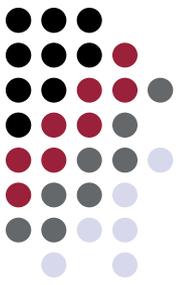
Tecnologias e Ferramentas para a Segurança da Informação



- 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

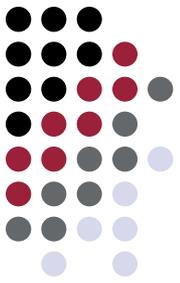


- Firewall

- Combinação de hardware e software que controla o fluxo de tráfego 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;

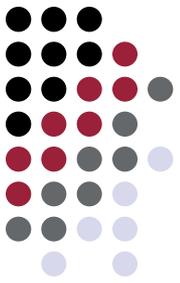


Tecnologias e Ferramentas para a Segurança da Informação



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

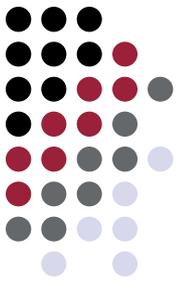
Tecnologias e Ferramentas para a Segurança da Informação



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

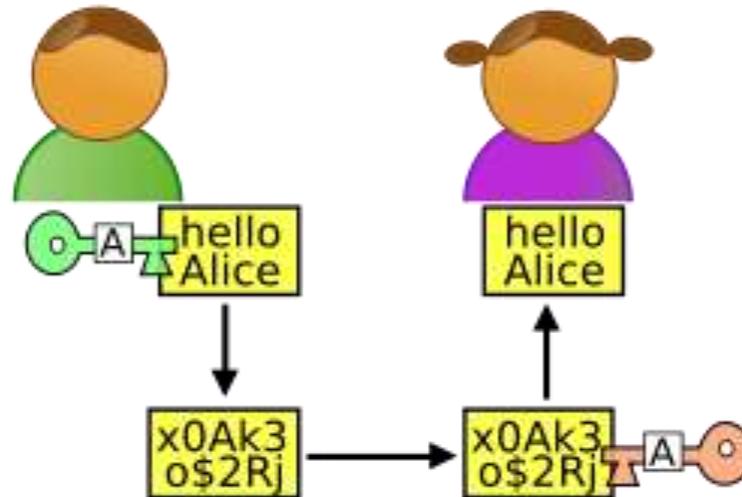


Tecnologias e Ferramentas para a Segurança da Informação

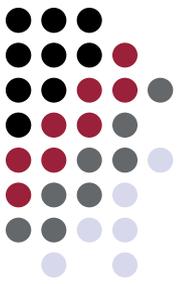


- Criptografia

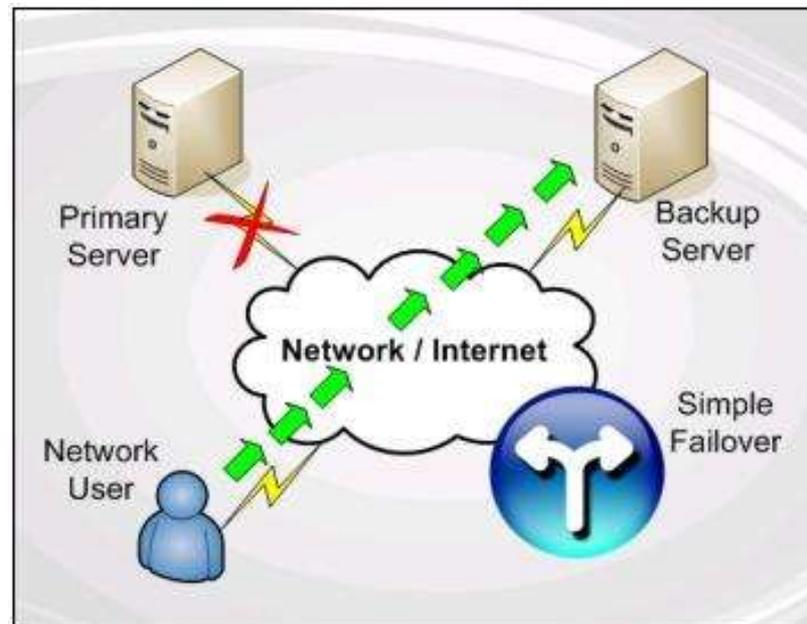
- Processo de transformar textos comuns ou dados em texto cifrado, legível somente ao destinatário



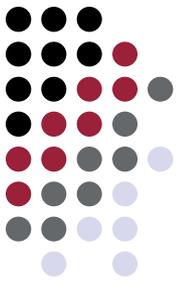
Tecnologias e Ferramentas para a Segurança da Informação



- 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

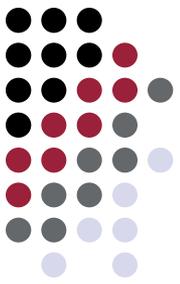


Aspectos Humanos da Segurança da Informação



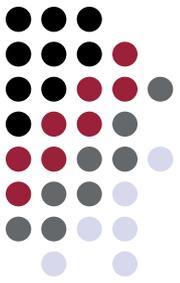
- Apesar de algumas tecnologias colaborarem para a segurança da informação, o usuário continua sendo um elemento chave
 - Engenharia Social
 - Hackers se passam por outras pessoas para conquistar informações dos usuários
 - Os usuários devem ter conhecimento sobre algumas práticas de hackers e pessoas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

Aspectos Humanos da Segurança da Informação

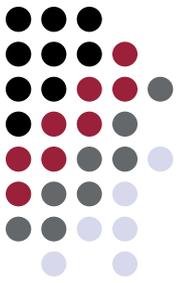


- Um caso recente
 - Professora perde R\$ 10 mil em golpe da página clonada do Banco do Brasil
 - <http://g1.globo.com/al/alagoas/noticia/2013/03/professora-perde-r-10-mil-em-golpe-da-pagina-clonada-do-banco-do-brasil.html>





- 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.



- *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

