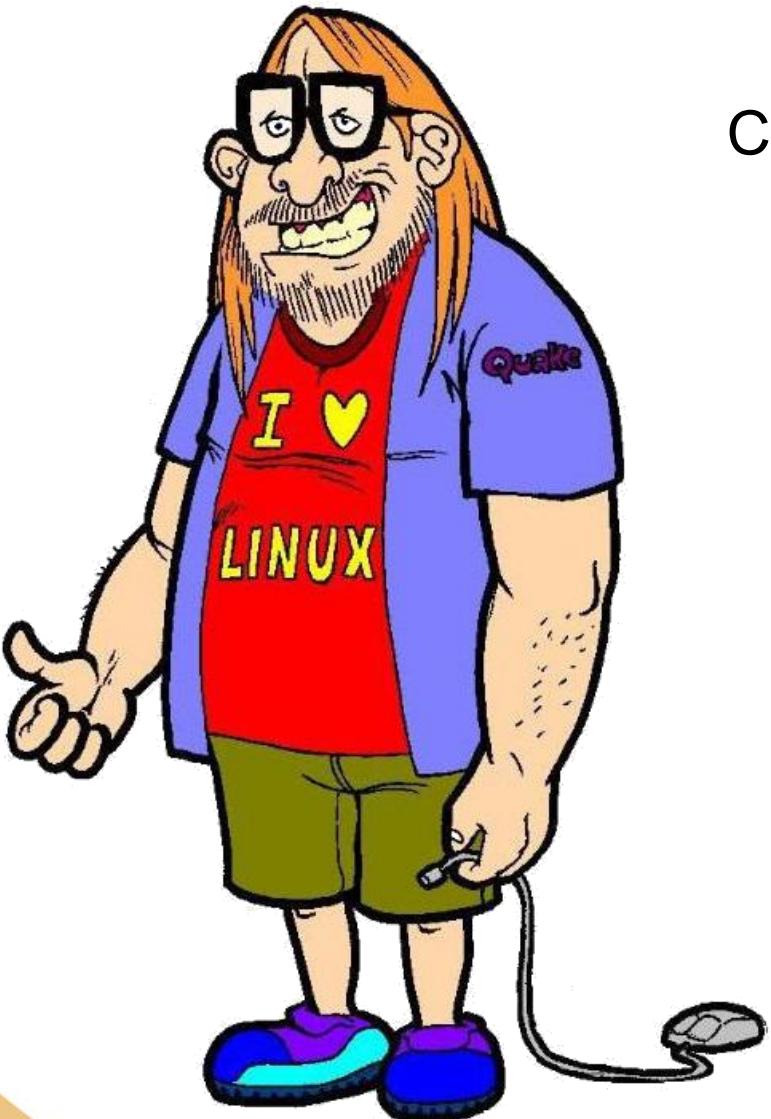


# **Segurança da Informação**

## **Sua empresa está segura na internet? é você???**

Prof. Robson Vaamonde  
SENAC Tatuapé



## Prof. Robson Vaamonde

Consultor de Infraestrutura de Redes de Computadores há 18 anos, técnico e tecnólogo em Redes de Computadores pelo Senac São Paulo (TATUAPÉ) e Faculdade FIAP. É certificado Microsoft Windows, GNU/Linux, CISCO e Furukawa, **especialista em interoperabilidade** entre plataformas operacionais e serviços de redes, docente do Senac Tatuapé e mantenedor dos blogs e redes sociais

**Procedimentos em TI e Bora para Prática.**

# Contatos



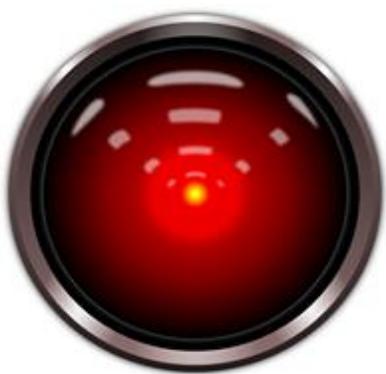
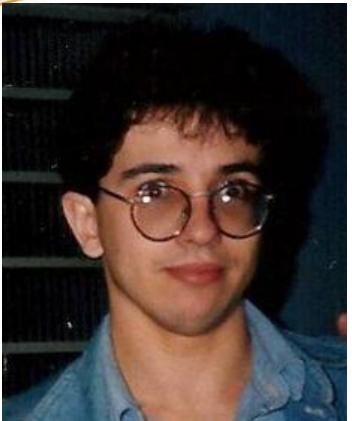
[facebook.com/ProcedimentosEmTi](https://facebook.com/ProcedimentosEmTi)



[facebook.com/boraparapratica](https://facebook.com/boraparapratica)



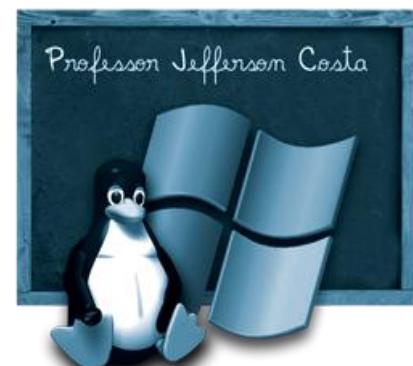
[youtube.com/user/boraparapratica](https://youtube.com/user/boraparapratica)



**Profº. José de Assis**  
Profissional da área de TI,  
atuando em  
Hardware, Redes, Java,  
soluções GNU/Linux e  
Robótica.  
[www.joseassis.com.br/](http://www.joseassis.com.br/)



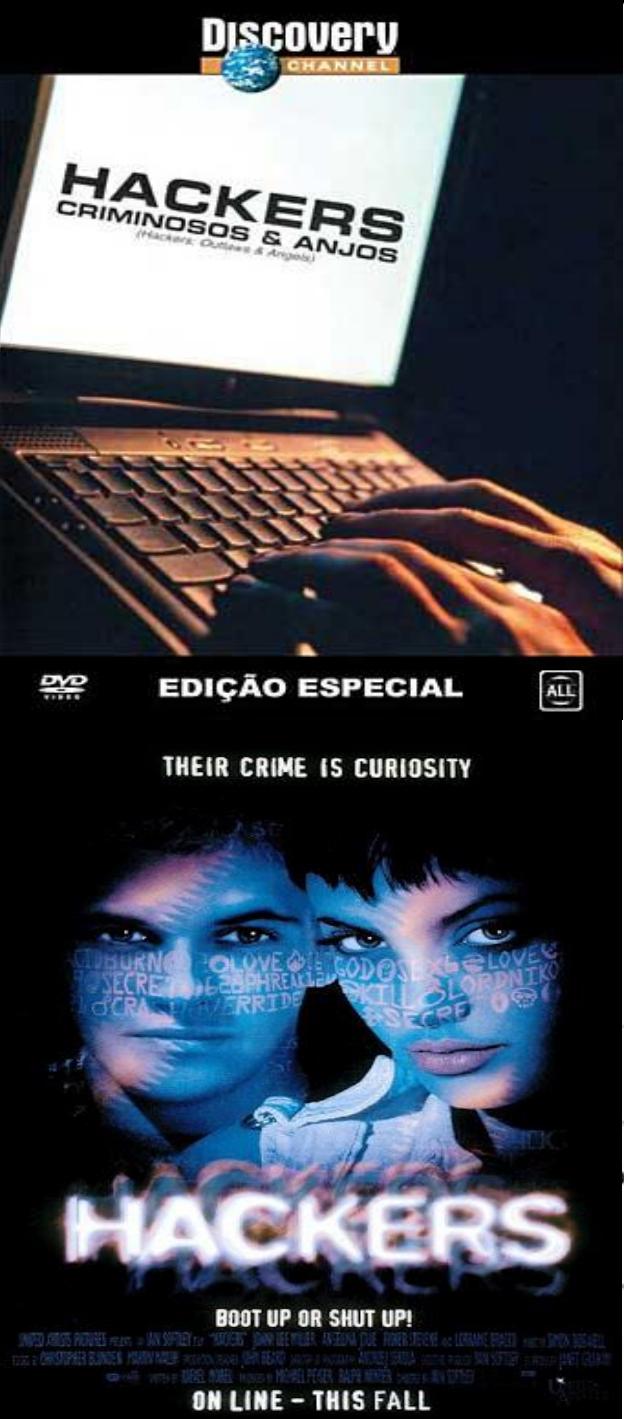
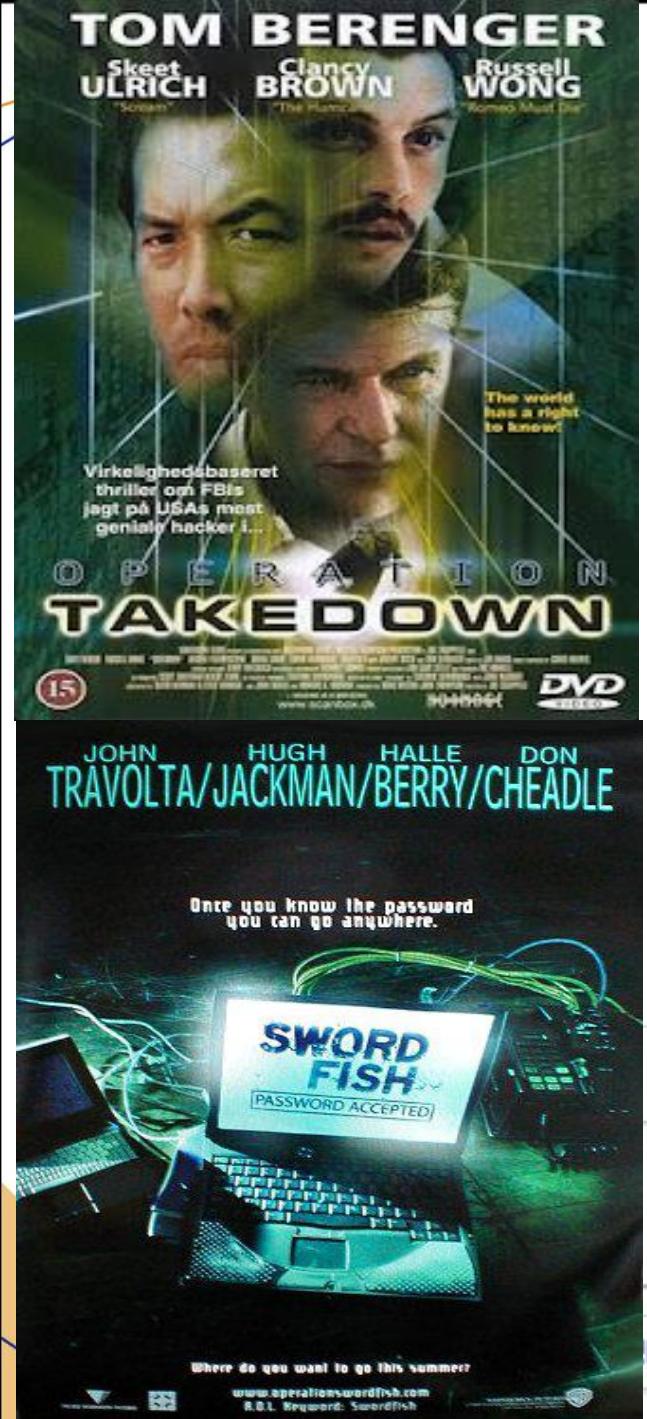
**Profº. Leandro Ramos**  
Profissional da área de TI,  
atuando em  
Hardware, Redes,  
Cabeamento e soluções  
Microsoft.  
[www.professorramos.com](http://www.professorramos.com)



**Profº. Jefferson Costa**  
Profissional da área de TI,  
atuando em segurança da  
informação, análise forense e  
soluções GNU/Linux e  
Microsoft.  
[www.jeffersoncosta.com.br](http://www.jeffersoncosta.com.br)



Profissionais altamente qualificados, equipe  
selecionada e treinada.



# Agenda

Panorama da Segurança da Internet, os principais Golpes e Ataques na Internet, Códigos Maliciosos, Spam, Riscos e Mecanismos de Segurança muito mais.....

# Estrutura do CGI.br



- 01- Ministério da Ciéncia e Tecnologia
- 02- Ministério das Comunicações
- 03- Casa Civil da Presidéncia da República
- 04- Ministério do Planejamento, Orçamento e Gestão
- 05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
- 06- Ministério da Defesa
- 07- Agênciá Nacional de Telecomunicações
- 08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
- 09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciéncia e Tecnologia

- 10- Notório Saber
- 11- Provedores de Acesso e Conteúdo
- 12- Provedores de Infra-estrutura de Telecomunicações
- 13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
- 14- Empresas Usuárias
- 15-18- Terceiro Setor
- 19-21- Academia

# Informação

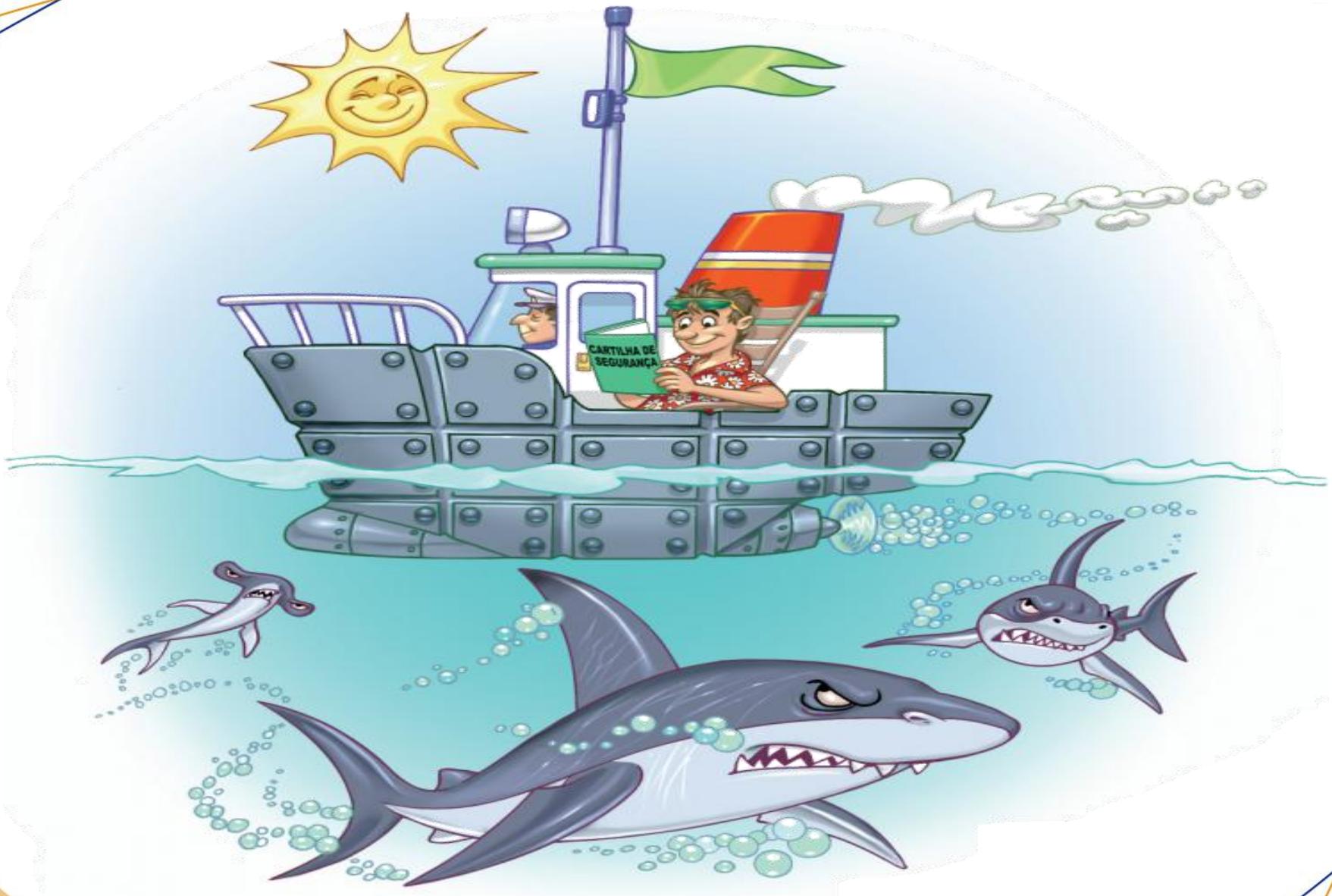
1. Qual o principal problema de segurança?
2. O quê deve ser protegido?
3. Quais os dados a serem protegidos?
4. Qual recurso utilizar?
5. Contra que ou quem vou proteger os meus dados?
6. Quais as ameaças mais prováveis?
7. Qual o grau de proteção desejado?
8. Quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança?
9. Quais as ocorrências em caso de incidência?
10. Qual a importância de cada recurso?



# Ativo da Informação

A informação é elemento essencial para todos os processos de negócio da organização, sendo portanto, um bem ou ativo de grande valor.





**Navegar é preciso,  
mais com segurança.**

# Segurança na Internet



A Internet ja está presente no cotidiano de grande parte da população e, provavelmente para estas pessoas, seria muito difícil imaginar como seria a vida sem poder usufruir das diversas facilidades e oportunidades trazidas por esta tecnologia.

# Segurança na Internet - Vantagens



- encontrar antigos amigos;
- acessar sites de notícias e de esportes;
- efetuar serviços bancários;
- fazer compras em supermercados e em lojas de comércio eletrônico;
- acessar sites dedicados a brincadeiras, etc;
- enviar a sua declaração de Imposto de Renda;
- consultar a programação das salas de cinema;
- consultar acervos de museus e sites dedicados a obra de grandes artistas.

# Segurança na Internet - Riscos

- Acesso a conteúdos impróprios ou ofensivos;
- Contato com pessoas mal-intencionadas;
- Furto de identidade;
- Furto e perda de dados;
- Invasao de privacidade;
- Divulgação de boatos;
- Dificuldade de exclusao;
- Dificuldade de detectar e expressar sentimentos;
- Dificuldade de manter sigilo;
- Uso excessivo;
- Plágio e violação de direitos autorais.



# Golpes na Internet



Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários.

# Golpes na Internet



- Furto de identidade (Identity theft);
- Fraude de antecipação de recursos (Advance fee fraud);
- Phishing (phishing-scam ou phishing/scam - engenharia social);
- Pharming (tipo específico de phishing, alteração do DNS);
- Golpes de comércio eletrônico;
- Boato (Hoax - conteúdo alarmante ou falso);

# Ataques na Internet



Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso a Internet pode participar de um ataque.

# Ataques na Internet - Motivação



- Demonstração de poder;
- Prestígio;
- Motivações financeiras;
- Motivações ideológicas;
- Motivações comerciais.

# Ataques na Internet - Famosos



Mark Abene (EUA): especialista em invasão de sistemas telefônicos, rede pública de telefonia.



Kevin Poulsen (EUA): também especializado em telefonia, ganhava concursos em rádios.



Robert Morris (EUA)  
Espalhou um vírus (worm) que infectou milhões de computadores e fez boa parte da Internet parar em 1998



Kevin David Mitnick (EUA)  
**O mais famoso HACKER do mundo.** Atualmente em liberdade condicional, foi condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas.  
**Os danos materiais são incalculáveis.** É uma lenda viva.  
Possui um site em [www.kevinmitnick.com](http://www.kevinmitnick.com).

# Ataques na Internet - Formas



- Exploração de vulnerabilidades;
- Varredura em redes (Scan - fping);
- Falsificação de e-mail (E-mail spoofing - hotmail);
- Interceptação de tráfego (Sniffing - Wireshark);
- Força bruta (Brute force - hydra);
- Desfiguração de página (Defacement);
- Negação de serviço (DoS e DDoS - ping of death)

# Códigos Maliciosos



Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador.

# Códigos Maliciosos - Formas



- Vírus (por e-mail, script, macro, telefone celular);
- Worm (propaga automaticamente);
- Bot ou Botnet (comunicação com o invasor)
- Spyware (minitorar atividades);
- Keylogger (captura teclas);
- Screenlogger (captura telas);
- Adware (propagandas);
- Backdoor (serviços e portas);
- Cavalo de Troia (funções escondidas);
- Rootkit (Kit de ferramentas do invasor);

# Spam



Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail).

# Spam - Formas - Técnicas



- Perda de mensagens importantes;
- Conteúdo impróprio ou ofensivo;
- Gasto desnecessário de tempo;
- Não recebimento de e-mails;
- Classificação errada de mensagens;
- Impacto na banda;
- Má utilização dos servidores;
- Inclusão em listas de bloqueio;
- Investimento extra em recursos;

## Técnicas de Spam

- Ataques de dicionário;
- Códigos maliciosos;
- Harvesting (pegar e-mail em páginas web)

# Outros Riscos



Atualmente, devido à grande quantidade de serviços disponíveis, a maioria das ações dos usuários na Internet são executadas pelo acesso a páginas Web, seja pelo uso de navegadores ou de programas leitores de e-mails com capacidade de processar mensagens em formato HTML.

# Outros Riscos - Formas



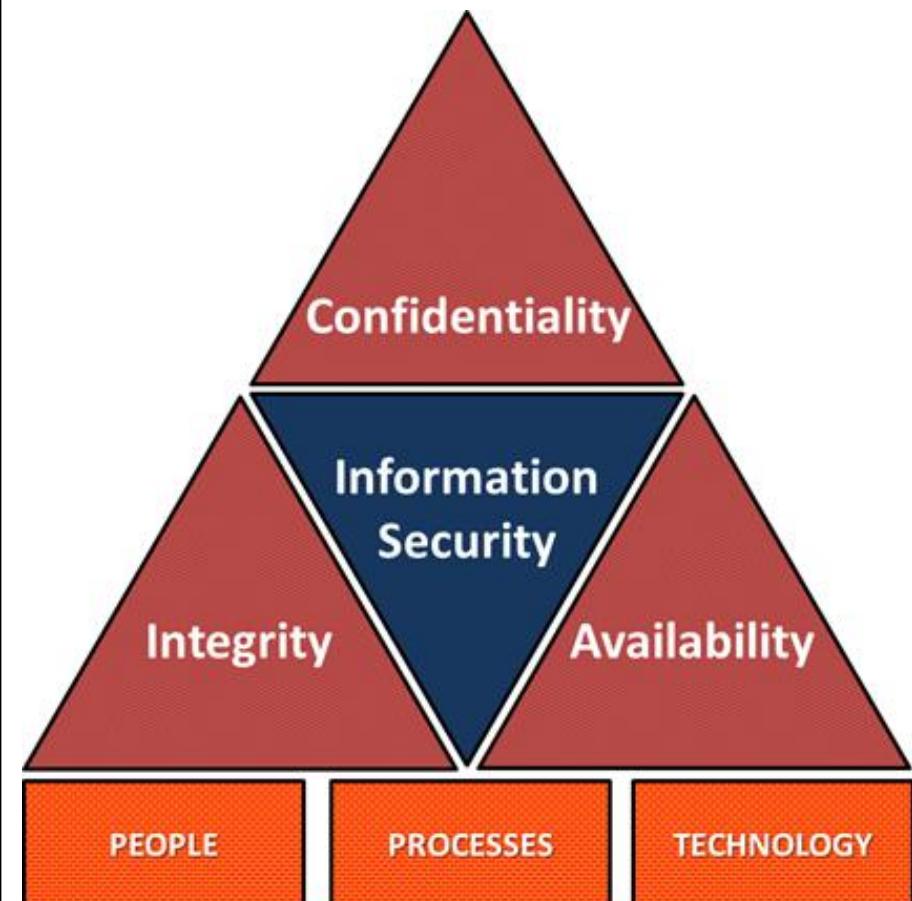
- **Cookies** (informações gravadas - autenticação, dados pessoais, etc);
- **Códigos Móveis** (funcionalidades, applets java, JavaScript, ActiveX, etc);
- **Janelas de Pop-Up** (mensagens indesejadas, links, cliques);
- **Plug-ins** (complementos para navegador);
- **Links Patrocinados** (anúncios pagos, páginas phishing);
- **Banners Propagandas** (banner mal-intencionados - malvertising);
- **Programas P2P**  
(compartilhamento de arquivos);
- **Compartilhamento de Recursos**  
(diretório, disco, impressora);

# Mecanismo de Segurança



Agora que você já está ciente de alguns dos riscos relacionados ao uso de computadores e da Internet e que, apesar disso, reconhece que não é possível deixar de usar estes recursos, está no momento de aprender detalhadamente a se proteger.

# Mecanismo de Segurança - Formas



- **Identificação:** permitir que uma entidade se identifique, ou seja, diga quem ela é
- **Autenticação:** verificar se a entidade é realmente quem ela diz ser.
- **Autorização:** determinar as ações que a entidade pode executar.
- **Integridade:** proteger a informação contra alteração não autorizada.
- **Confidencialidade** ou sigilo: proteger uma informação contra acesso não autorizado.
- **Não repúdio:** evitar que uma entidade possa negar que foi ela quem executou uma ação.
- **Disponibilidade:** garantir que um recurso esteja disponível sempre que necessário.

# Características fundamentais da informação

- **Confidencialidade:** É quando as pessoas são autorizadas a terem acesso a informação.
- **Integridade:** É quando a informação está completa, sem ter sofrido alterações e, portanto, confiável.
- **Disponibilidade:** É quando a informação está acessível, por pessoas autorizadas, sempre que necessário.
- **Autenticidade:** É quando a autenticação é válida.



# Política de Segurança da Informação - Formas



- **Política de senhas:** define as regras sobre o uso de senhas;
- **Política de backup:** define as regras sobre a realização de cópias de segurança;
- **Política de privacidade:** define como são tratadas as informações pessoais;
- **Política de confidencialidade:** define como são tratadas as informações institucionais;
- **Política de uso aceitável (PUA) ou Acceptable Use Policy (AUP):** também chamada de “Termo de Uso” ou “Termo de Serviço”.

# Vulnerabilidades

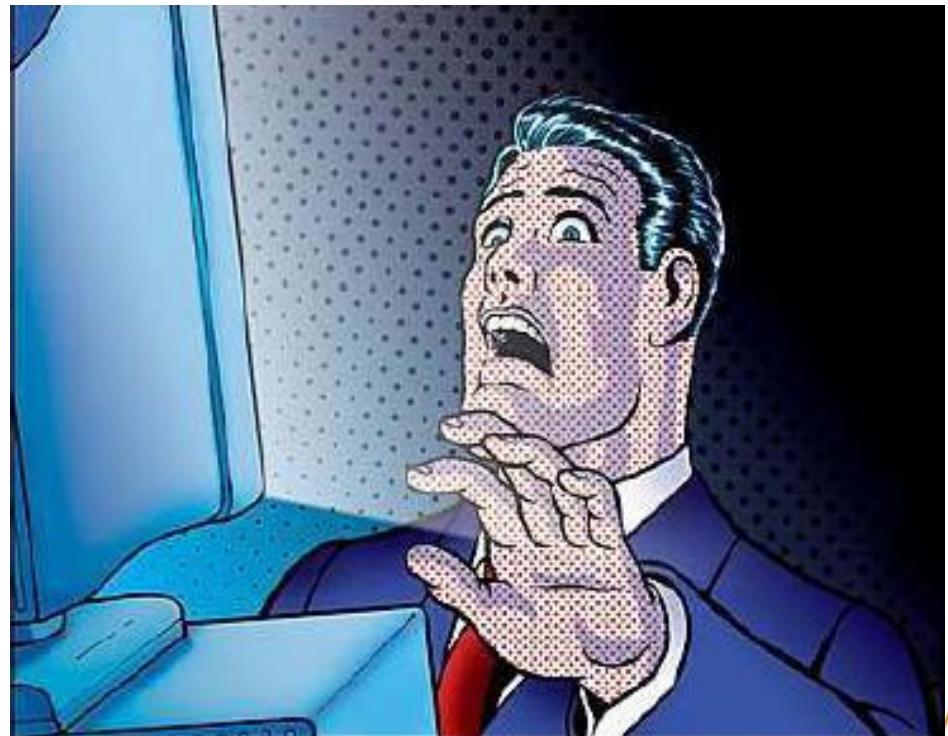
São as fraquezas presentes nos ativos da informação, podendo causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação:

**CONFIDENCIALIDADE,**  
**INTEGRIDADE,** e  
**DISPONIBILIDADE.**



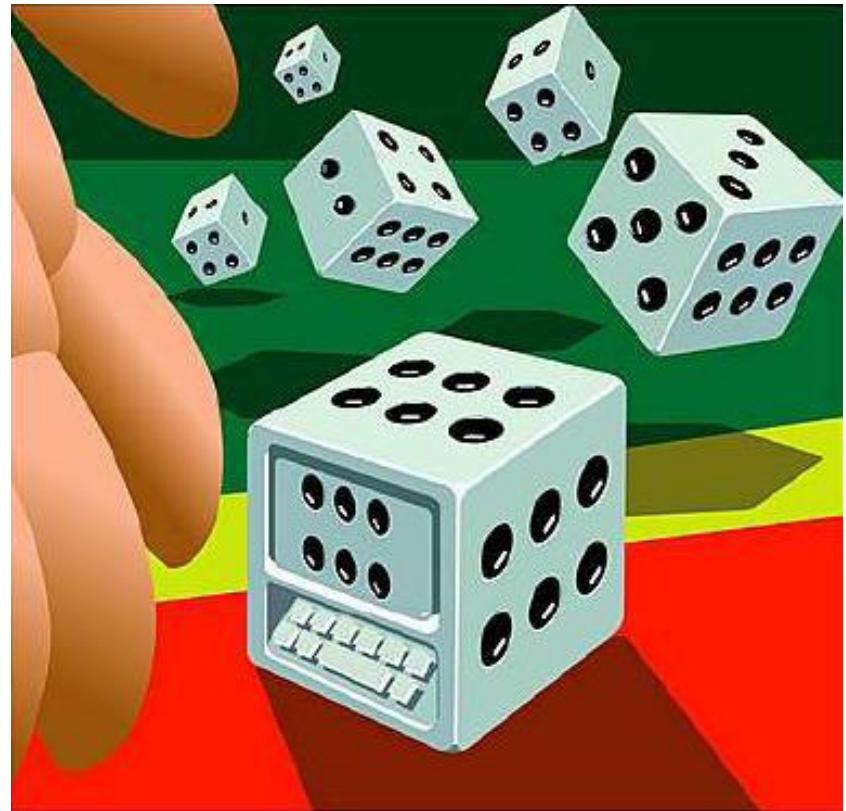
# Ameaças

A ameaça é um agente externo ao ativo de informação, que poderá quebrar a confidencialidade, integridade ou disponibilidade da informação.



# Probabilidade

É a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos.



# Impacto

São as  
conseqüências  
que este  
incidente possa  
causar a  
organização.

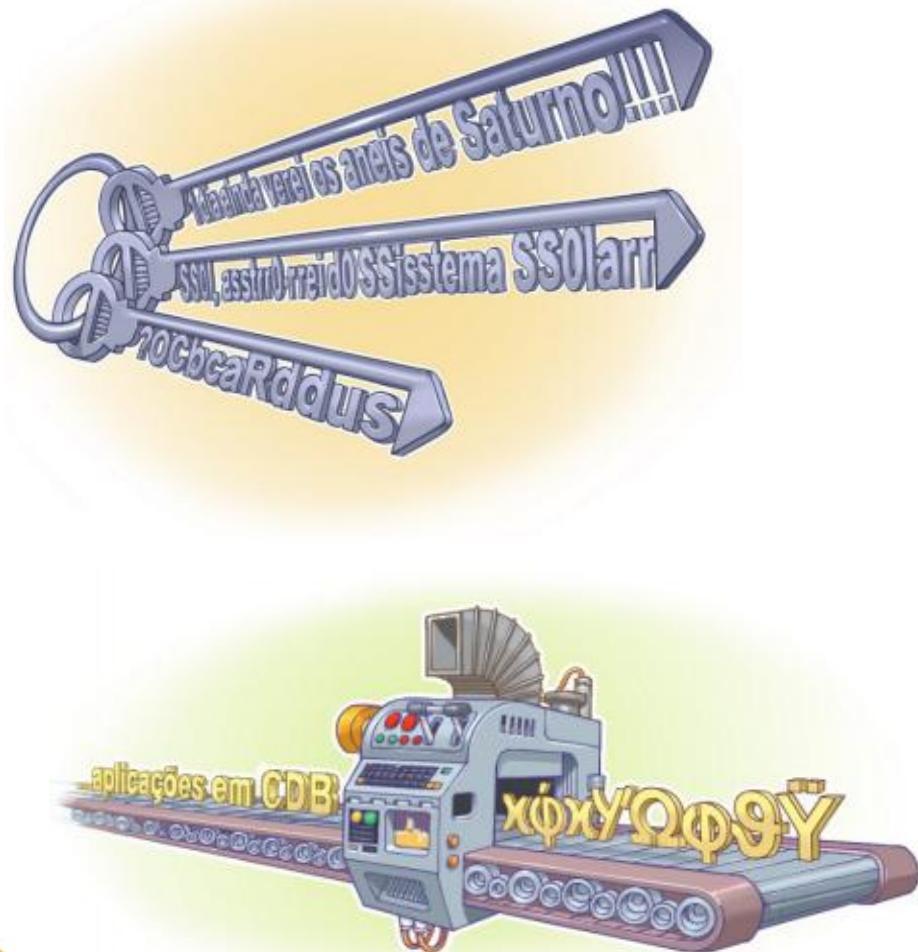


# Risco

**RISCO = IMPACTO \* PROBABILIDADE**

O risco é a relação entre a probabilidade e o impacto. É a base para a identificação dos pontos que demandam por investimentos em segurança da informação

# Senhas, Criptografia, Backups - Formas



- **Contas e senhas** são atualmente o mecanismo de autenticação mais usado para o controle de acesso a sites e serviços oferecidos pela Internet;
- **Criptografia** você pode proteger seus dados contra acessos indevidos, tanto os que trafegam pela Internet como os já gravados em seu computador.
- **Cópias de segurança (Backups)**, Proteção de dados, Recuperação de versões, Arquivamento, Onde gravar os backups, Quais arquivos copiar, Com que periodicidade devo realizá-los.

# Ferramentas de Segurança - Formas



Sites:

<https://noscript.net/>

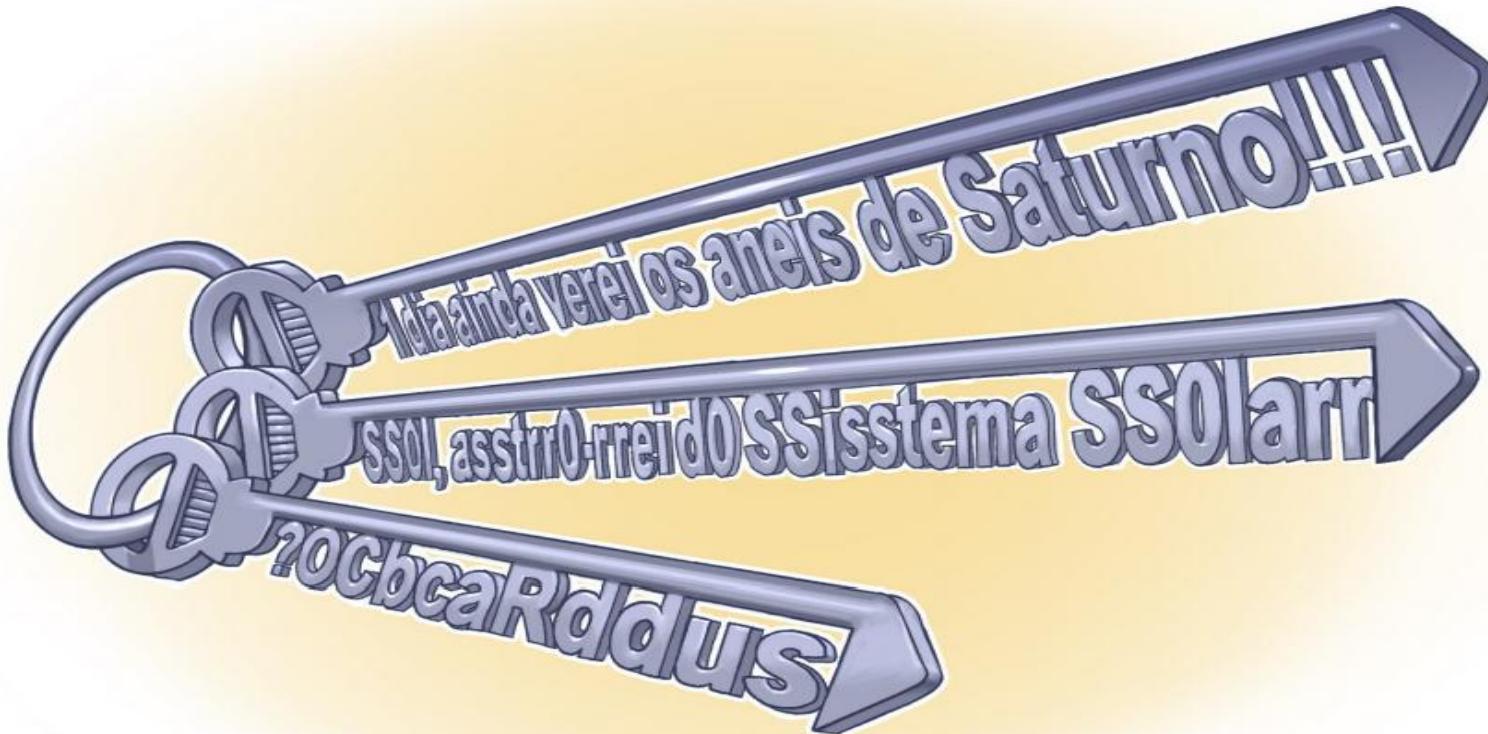
<https://adblockplus.org/>

<https://www.mywot.com/>

<https://www.anonymizer.com/>

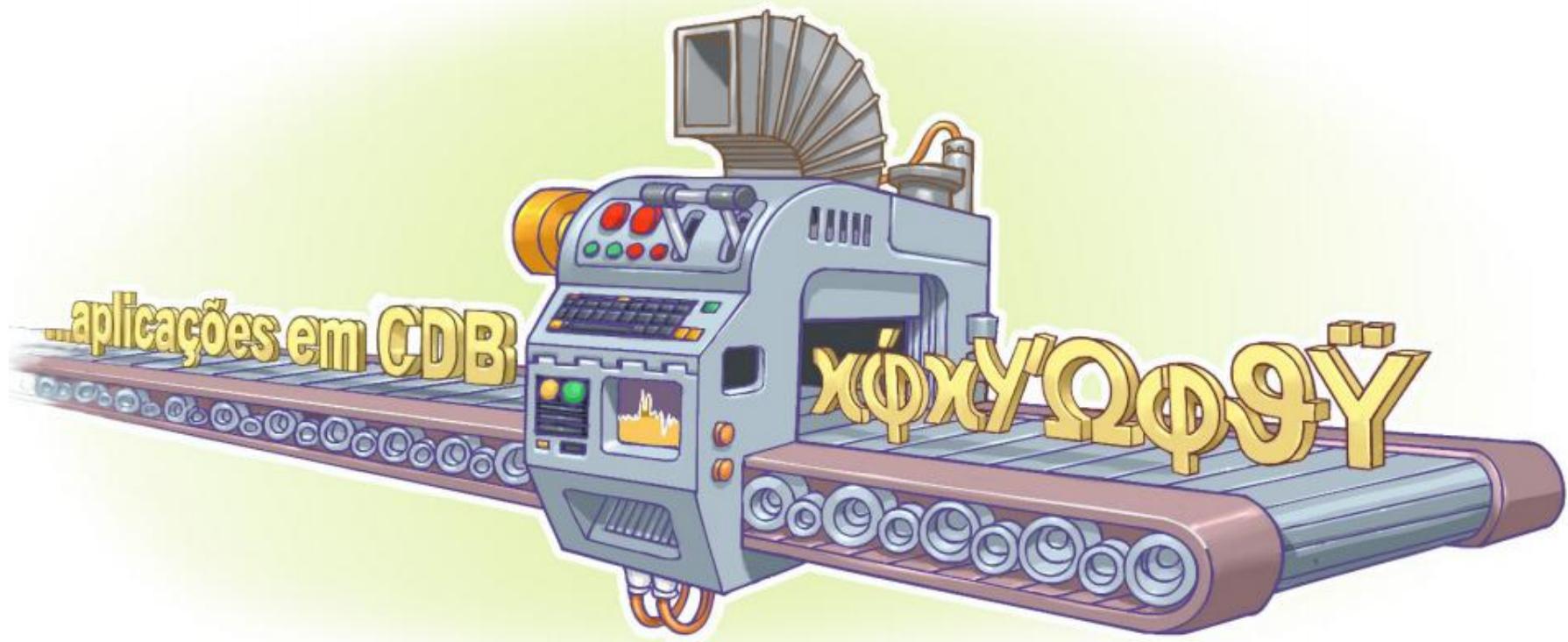
- **Ferramentas anti-malware:** Método de detecção, Forma de obtenção, Execução, Funcionalidades apresentadas;
- **Firewall pessoal:** registrar as tentativas de acesso, bloquear envio de informações, bloquear tentativas de invasão, análise de acesso e navegação;
- **Filtro Antispam:** habilitar nos Webmail e Gerenciadores de E-mail;
- **Outros Mecanismos:** Filtro antiphishing, Filtro de janelas de pop-up, Filtro de códigos móveis, Filtro de bloqueio de propagandas, Teste de reputação de site, Programa para verificação de vulnerabilidades,

# Contas e Senhas



Uma conta de usuário, também chamada de “nome de usuário”, “nome de login” e username, corresponde a identificação única de um usuário em um computador ou serviço.

# Criptografia



...aplicações em CDB

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

# **Criptografia - Exemplo 1/4**

**Sejam Bem-Vindos ao SENAC  
Tatuapé**

**Palestra Segurança da  
Informação**

**Texto não Criptografado**

# Criptografia - Exemplo 2/4

S3j4m B3m-V1nd0s 40

S3N4C T4t54p3

P4l3str4 S3g5r4nç4 d4

1nf0rm4ç40

T3xt0 n40

Cr1pt0gr4f4d0

Referência:

A = 4

E = 3

I = 1

O = 0

U = 5

# Criptografia - Exemplo 3/4

S3j4m%B3m-  
V1nd0s%40%S3N4C%T4t  
54p3

P4l3str4%S3g5r4nç4%d4%  
1nf0rm4ç40

T3xt0%n40%Cr1pt0gr4f4d0

Referência:

A = 4

E = 3

I = 1

O = 0

U = 5

Barra de espaço = %

# Criptografia - Exemplo 4/4

&S3j4m%B3m-  
v1nd0s%40%S3N4C  
%T4t54p3\$&P4I3str4  
%S3g5r4nç4%d4%1nf  
0rm4ç40\$&T3xt0%n4  
0%Cr1pt0gr4f4d0\$

Referência:

A = 4

E = 3

I = 1

O = 0

U = 5

Barra de espaço = %

Início paragrafo = &

Quebra de linha

ou Fim paragrafo = \$

# Criptografia - Desafio

VDLKSDFJOW45340985LDLKSDFJOW45340985P  
OSDKFJHSDF8934466ESDKFJHSDF8934466A  
CFDKGAS843432257SDRFDKGAS843432257SDR  
ÊUQWE0I945834=-0545EUQWE0I945834=-0545A  
CLDKJSLDJG499830911SLDKJSLDJG499830911B  
OSDGG465345GDGFG5SSDGG465345GDGFG5É  
NRERT634634534GER1ARERT634634534GER1N  
SDFHRY5634634T34T31FDFHRY5634634T34T31S  
EKSIE300LKJTW535935RKSIE300LKJTW535935!  
GKIEEDSIWEOPRIWPOAKIEEDSIWEOPRIWPO!  
UDÇLKERIWOEPWER3SDÇLKERIWOEPWER3!  
ESDFOSIFPEOP543232ESDFOSIFPEOP543232!

# Criptografia - Resposta

**V**DLKSDFJOW45340985**L**DLKSDFJOW45340985**P**

**O**SDKFJHSDF8934466**E**SDKFJHSDF8934466**A**

**C**FDKGAS843432257SD**R**FDKGAS843432257SD**R**

**Ê**UQWEI945834=-0545**E**UQWEI945834=-0545**A**

**C**LDKJSLDJG499830911**S**LDKJSLDJG499830911**B**

**O**SDGG465345GDGFG5**S**SDGG465345GDGFG5**É**

**N**RERT634634534GER1**A**RERT634634534GER1**N**

**S**DFHRY5634634T34T31**F**DFHRY5634634T34T31**S**

**E**KSIE300LKJTW535935**R**KSIE300LKJTW535935**!**

**G**KIEEDSIWEOPRIWPO**A**KIEEDSIWEOPRIWPO**!**

**U**ĐÇLKERIWOEPWER3**S**ĐÇLKERIWOEPWER3**!**

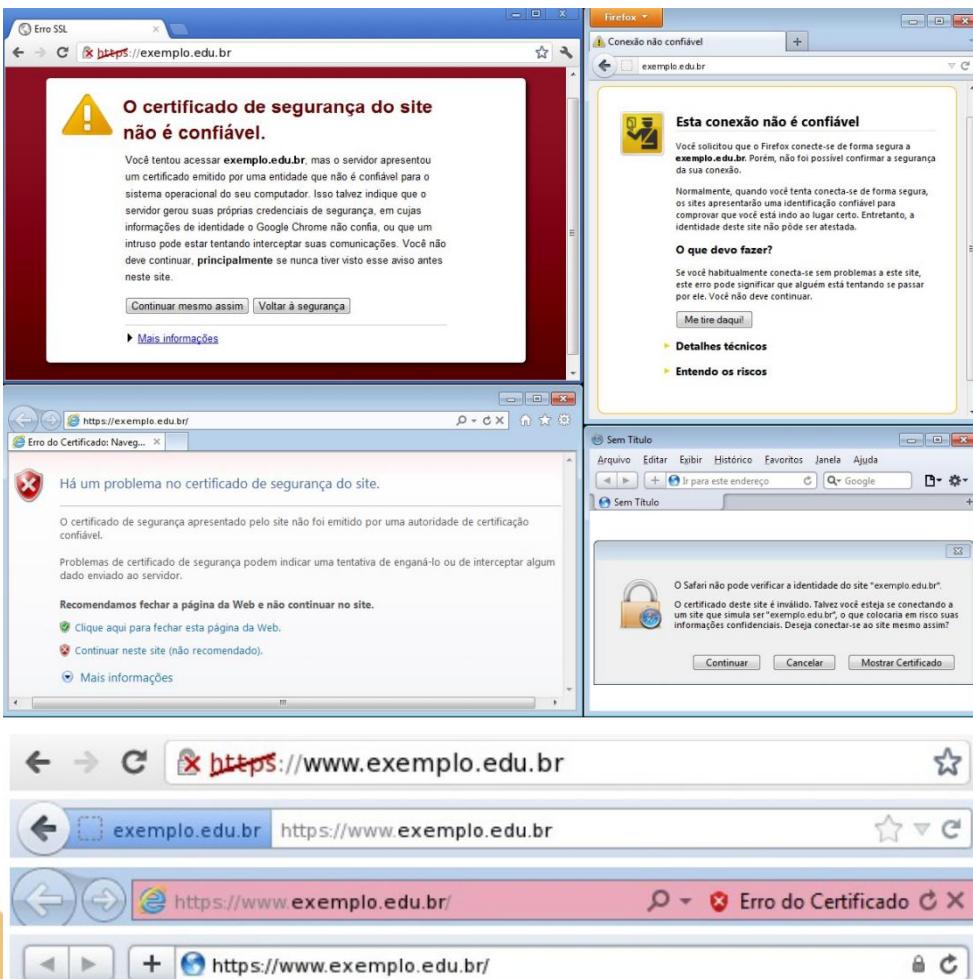
**E**SDFOSIFPEOP543232**E**SDFOSIFPEOP543232**!**

# Uso seguro da Internet



A Internet traz inúmeras possibilidades de uso, porém para aproveitar cada uma delas de forma segura é importante que alguns cuidados sejam tomados.

# Uso seguro da Internet - Formas



- **Navegadores de WEB:** manter atualizados, complementos conhecidos, cuidado com o JavaScript, etc;
- **Leitores de E-mail:** MS Outlook, Thunderboard, etc;
- **Webmails:** cuidados ao abrir webmails em qualquer lugar;
- **Transações Bancárias:** certificado, site de busca, por e-mail, etc;
- **Compras On-Line:** lojas on-line, cartão de crédito, dados pessoais, etc;
- **Segurança de Acesso:** HTTP ou HTTPS, SSL, etc, confiabilidade do certificado digital;

# Privacidade



Nada impede que você abdique de sua privacidade e, de livre e espontânea vontade, divulgue informações sobre você. Entretanto, há situações em que, mesmo que você queira manter a sua privacidade, ela pode ser exposta independente da sua vontade

# Privacidade - Formas



- Acessar e armazenar seus e-mails: configurar navegador/leitor de e-mails;
- Acessar é utilizar navegadores de Web: Lan-house, cyber-café, etc;
- Divulgação de informações na Web: muito cuidado!!!!

# Privacidade - Redes Sociais



- **Contato com pessoas mal-intencionadas:** qualquer pessoa pode criar um perfil falso;
- **Furto de identidade:** assim como você pode ter um impostor na sua lista de contatos;
- **Invasão de perfil:** por meio de ataque de força bruta;
- **Invasão de privacidade:** quanto maior a sua rede de contatos, maior e o número de pessoas que possui acesso ao que você divulga;
- **Vazamento de informações:** há diversos casos de empresas que tiveram o conteúdo de reuniões e detalhes técnicos de novos produtos divulgados na Internet;
- **Disponibilização de informações confidenciais:** em uma troca “amigável” de mensagens você pode ser persuadido a fornecer seu e-mail, telefone, etc

# Segurança de Computadores



Muito provavelmente e em seu computador pessoal que a maioria dos seus dados está gravada e, por meio dele, que você acessa e-mails e redes sociais e realiza transações bancárias e comerciais. Por isto, mantê-lo seguro é essencial para se proteger dos riscos envolvidos no uso da Internet.

# Segurança de Computadores



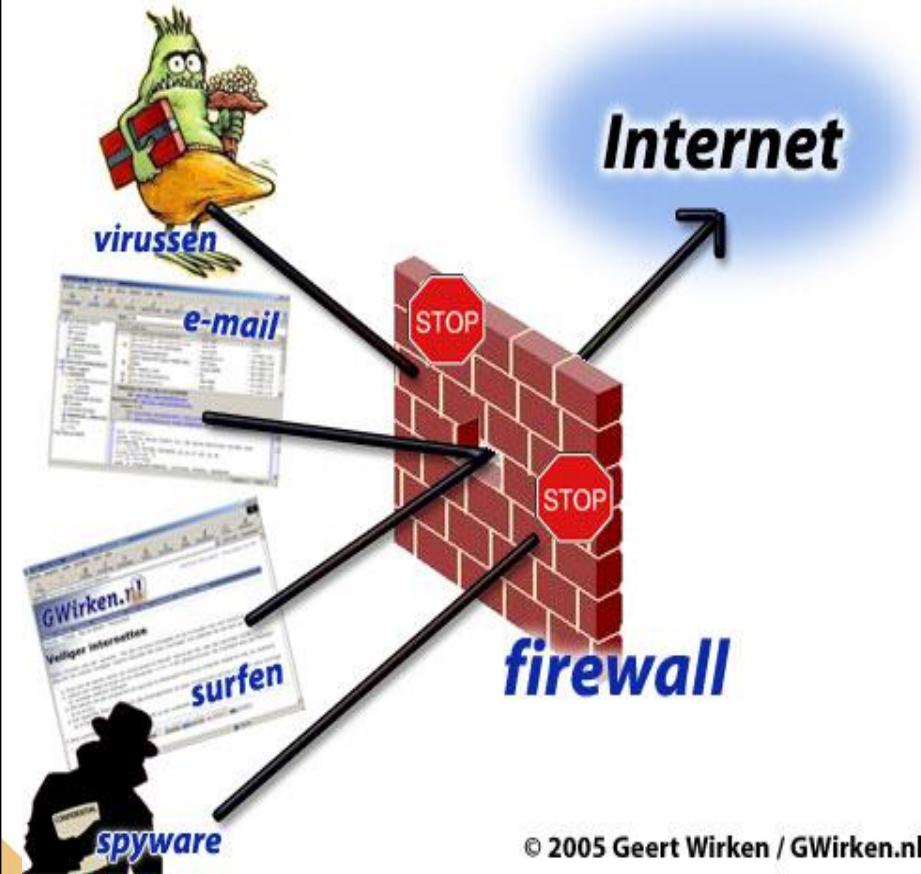
- Mantenha os programas instalados com as versões mais recentes:
- Mantenha os programas instalados com todas as atualizações aplicadas:
- Use apenas programas originais:
- Use mecanismos de proteção:
- Use as configurações de segurança já disponíveis:
- Seja cuidadoso ao manipular arquivos:
- Proteja seus dados:
- Mantenha seu computador com a data e a hora corretas:
- Crie um disco de recuperação de sistema:
- Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros:
- Seja cuidadoso ao enviar seu computador para serviços de manutenção:

# Segurança de Redes



Inicialmente, grande parte dos acessos à Internet eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um modem e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede.

# Segurança de Redes



© 2005 Geert Wirken / GWirken.nl

- Furto de dados;
- Uso indevido de recursos;
- Varredura;
- Interceptação de tráfego;
- Ataque de negação de serviço;
- Ataque de força bruta;
- Rede Wireless (WiFi);
  - Infraestrutura:
  - Ponto a ponto (ad-hoc);
  - WEP, WPA/2, SSID
  - Bluetooth
- Banda Larga;
- Banda Larga Móvel.

# Segurança de Dispositivos Móveis



Dispositivos móveis, como tablets, smartphones, celulares e PDAs, têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação Web, Internet Banking e acesso a e-mails e redes sociais.

# Segurança de Dispositivos Móveis



- Grande quantidade de informações pessoais armazenadas;
- Maior possibilidade de perda e furto;
- Grande quantidade de aplicações desenvolvidas por terceiros;
- Rapidez de substituição dos modelos;
- Proteja seu dispositivo móvel e os dados nele armazenados:

# Dúvidas?????



A collage of the words "thank you" in many different languages, arranged in a dense, overlapping cluster. The languages include English, Spanish, Portuguese, French, German, Italian, Dutch, Swedish, Danish, Norwegian, Polish, Czech, Hungarian, Russian, Chinese, Japanese, Korean, and others. Each word is rendered in a different font and size, creating a visually dense and international composition.



# 100% de Segurança é Utopia

“Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza sobre o primeiro”.

# *Albert Einstein*

# Méritos e Créditos da Palestra

Cgi.br: <http://cgi.br/>

Nic.br: <http://www.nic.br/>

Registro.br: <http://registro.br/>

Cert.br: <http://www.cert.br/>

Cartilha Cert.br: <http://cartilha.cert.br/>

Antispam.br <http://antispam.br/>

Internet Segura.br: <http://internetsegura.br/>

Kaspersky Real Time Stats: <http://kaspersky-cyberstat.com/>

Kaspersky Secure Password Check: <https://blog.kaspersky.com.br/password-check/>

10TopTenReviews: <http://software.toptenreviews.com/>

Hydra: <https://www.thc.org/>

Nmap: <https://nmap.org/>

Wireshark: <https://www.wireshark.org/>

OpenVAS: <http://www.openvas.org/>

LinSSID: <http://sourceforge.net/projects/linssid/>

Aircrack-ng: <http://www.aircrack-ng.org/>