Segurança da Informação

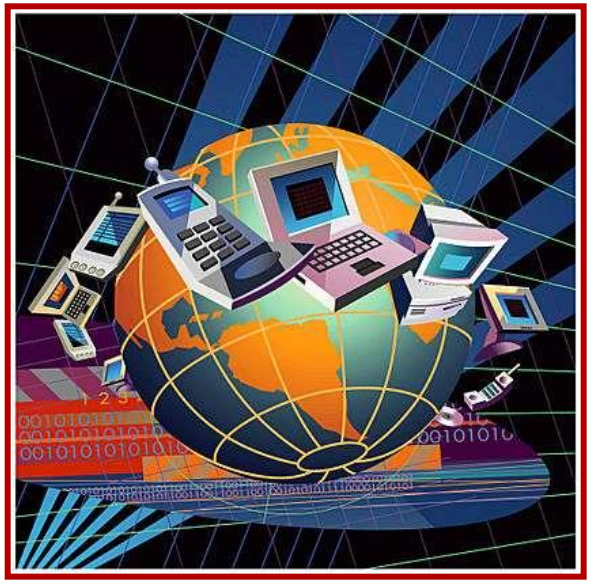
Givanaldo Rocha

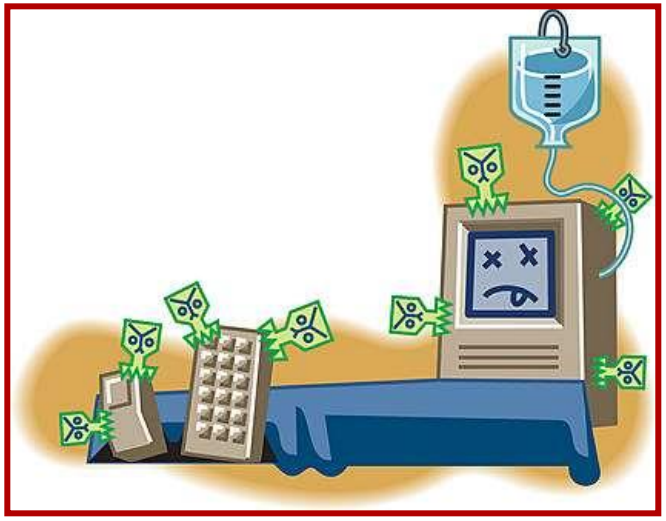
givanaldo.rocha@ifrn.edu.br

http://docente.ifrn.edu.br/givanaldorocha

Cenário Atual

- Era da Informação e da Globalização:
  - Avanços da Tecnologia da Informação;
  - Avanços nas Telecomunicações;
  - Maior rapidez na troca das informações;
  - Maior exigência das pessoas;
- Globalização das Ameaças.
- Novos Riscos e Vulnerabilidades:
  - Novos vírus surgem a cada momento;
  - Quebra de sigilo de informações confidenciais para benefício próprio ou para a concorrência.
  - Ataques virtuais tem comprometido a imagem das empresas.





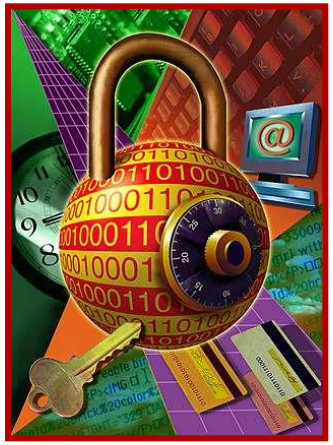
Informação

Classificação das informações:

- **Públicas**: podem ser disseminadas dentro e fora da empresa.
- **Corporativas**: devem ser disseminadas somente dentro da empresa.
- **Confidenciais**: devem ser disseminadas somente para empregados nomeados.
- **Secreta**: o acesso interno ou externo de pessoas não autorizadas a esse tipo de informações é extremamente crítica para a instituição.

Segurança da Informação

- A primeira ideia que se pensa é a proteção das informações, não importando onde estejam.
  - No papel, na memória do computador, em um disquete ou trafegando pela linha telefônica.
- A expectativa de todo o usuário é que as **informações armazenadas hoje no seu computador lá permaneçam**, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham acessado o seu conteúdo.
- O usuário espera que suas informações estejam no momento e local que ele determinar, que sejam confiáveis, corretas e mantidas fora do alcance e da vista de pessoas não autorizadas.

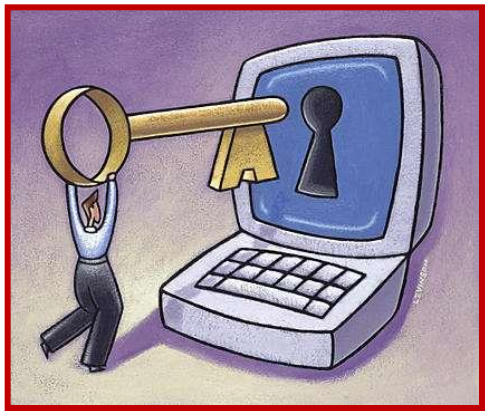


O que é Segurança da Informação?

- **Definição**:
  - Proteção dos sistemas de informação contra o acesso de usuários não autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, a fim de prevenir, detectar, deter e documentar eventuais ameaças ao seu desenvolvimento.

- **Segurança da Informação** é, de uma forma mais geral, a prevenção e redução dos riscos relacionados ao uso indevido da informação.

- Proteção das informações e dos conhecimentos sensíveis para a garantia de continuidade do negócio da empresa.



Medidas de Segurança da Informação

- Política de segurança da informação;
- Política de utilização da Internet e correio eletrônico;
- Política de instalação e utilização de softwares;
- Plano de classificação das informações;
- Auditoria;
- Análise de riscos;
- Análise de vulnerabilidades;
- Análise da política de backup;
- Capacitação técnica;
- Processo de conscientização dos usuários.

Política de Segurança da Informação

PSI

Política de Segurança da Informação

- Normas e diretrizes adotadas com a finalidade de proteger um ambiente, podendo ser computacional ou não.
- Ambiente computacional: proteção lógica e física, utilizando ferramentas necessárias para tais proteção.
- Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira).
- Em uma linguagem simples:
  - Deve especificar “o quê” e “por que” proteger ao invés de “como” isso vai ser implementado.

Política de Segurança da Informação

- Alguns pontos devem ser levados em consideração para a elaboração da Política de Segurança da Informação, entre eles:
  - O que deve ser protegido?
  - Contra quem/que será necessário proteger?
  - Como será feita a proteção e qual seu grau desejado?
  - Quais são as ameaças mais prováveis?
  - Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
  - Quanto vale a informação para a empresa?
  - Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

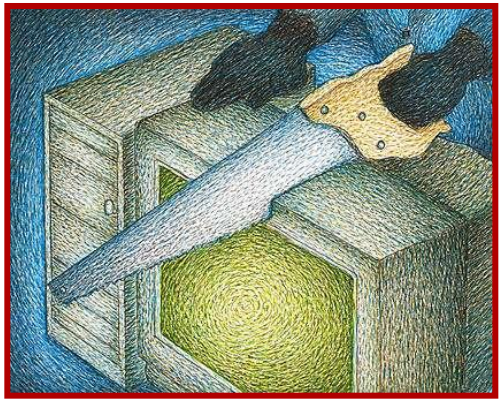
Objetivo da Política de Segurança

- Hoje em dia a informação é o ativo mais valioso das grandes empresas. Por isso, a política de segurança visa proteger a **informação**.
- É preciso se conscientizar da necessidade da criação e do cumprimento de uma Política de Segurança da Informação.
- Também é necessário viabilizar os recursos necessários para a criação e a manutenção.
- O objetivo da Política de Segurança é definir a forma da utilização dos seus recursos através de procedimentos para prevenir e atender incidentes de segurança.

Ameaças à Política de Segurança

- Ameaça pode ser:
  - Uma pessoa, uma coisa, um evento ou uma ideia capaz de causar dano a um recurso, em termos de confidencialidade, integridade, disponibilidade, etc.

- Análise das ameaças e vulnerabilidades deve levar em consideração todos os eventos adversos que podem explorar as fragilidades de segurança.



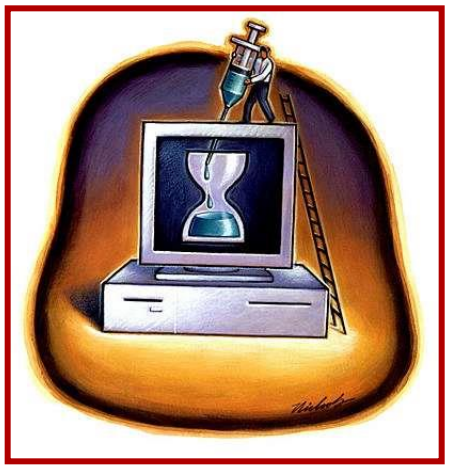
Divulgação da Política de Segurança

- Avisos;
- Reuniões;
- Treinamentos gerais e departamentais ou setoriais;
- Exemplificação através de informativos, jornais, peças teatrais e outros veículos de informação.

Se existe alguma política de segurança e as pessoas da organização não sabem, não serve para nada!!!

Controles Necessários

- Software de detecção de vírus
- Software de controle de acesso lógico
- Mecanismos de controle de acesso físico
- Política de *backup* (cópia de segurança)
- Política de uso de software
- Definição dos agentes envolvidos em segurança da informação



Política de Acessos Externos à Instituição

- Definição de convênios para acesso às bases corporativas
- Criptografia
- Certificação digital
- *Log* (registro) de acessos
- Configuração de *firewall*

Política de Backup

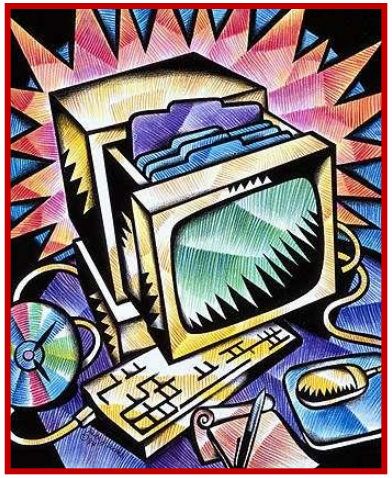
O que é um backup?

É uma cópia de segurança de arquivos, geralmente mantida em mídias removíveis (fitas magnéticas, pendrives, CD/DVD, HD Externo etc.), que permitem o resgate de informações importantes ou programas em caso de falha do disco rígido.

Por que fazer backup?

De alguma forma, quem trabalha com computador acaba um dia perdendo dados contidos no disco rígido, que pode sofrer danos e ficar inutilizado por inúmeros motivos.

A periodicidade de realização do backup deve ser definida de acordo com o volume de informação.

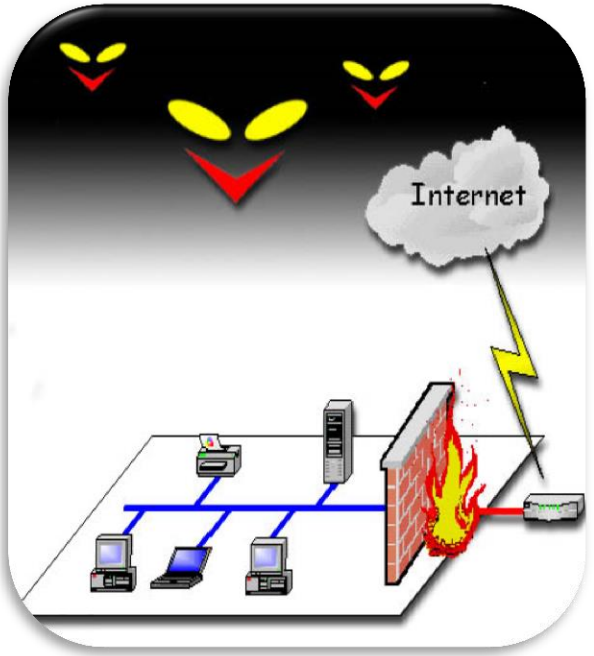


Segurança Externa do Backup

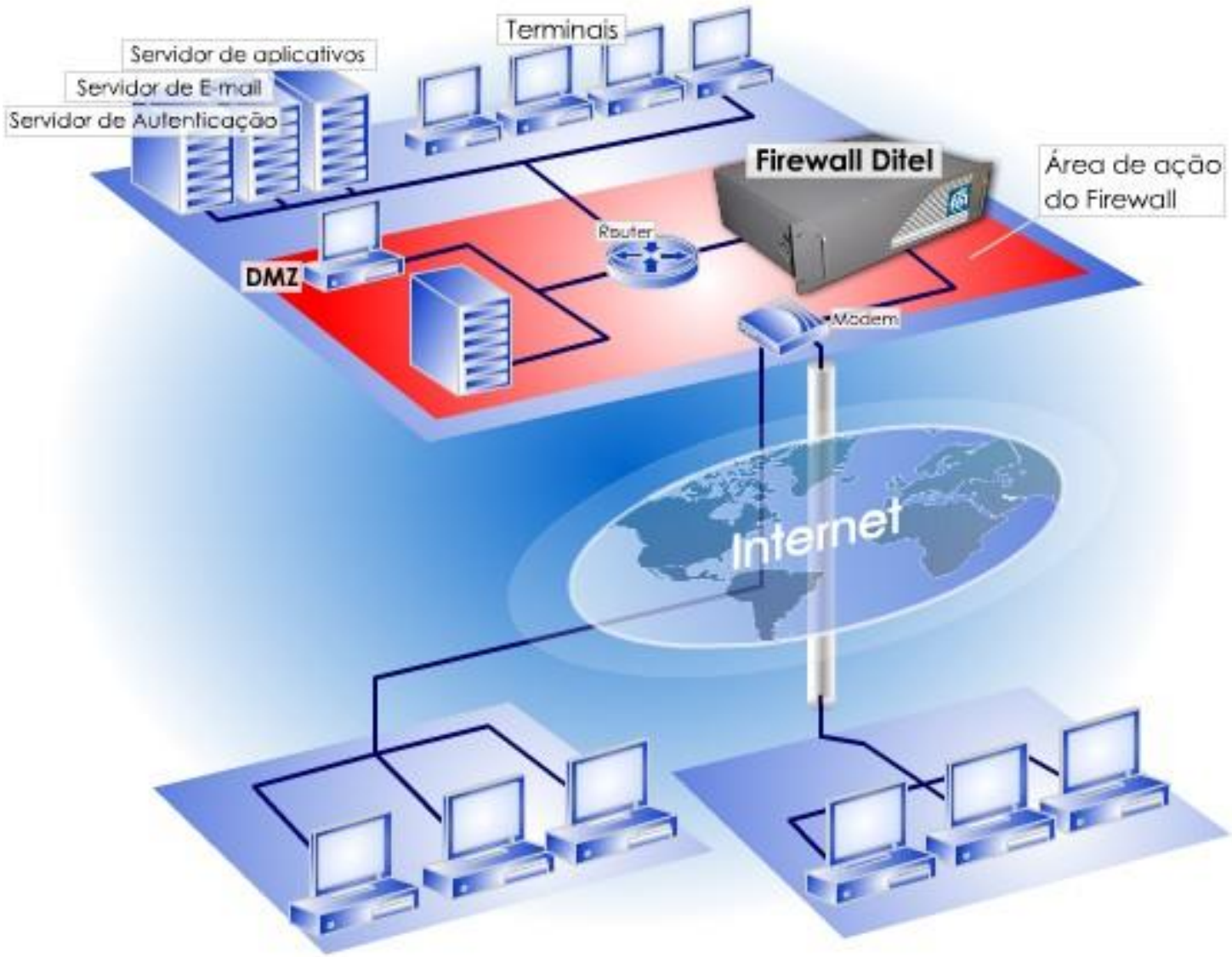
- Armazenar em local protegido de umidade, mofo e incêndio.
- Se o dado é de vital importância ter mais de uma cópia em locais diferentes.
- Manter rótulo nos backup para facilitar a identificação.
- Colocar em local de acesso restrito.

Firewall

- Filtra todo o tráfego entre a Internet e a rede local ou entre os computadores de uma rede local.
- Imprescindível para qualquer empresa de pequena ou média dimensão.
- Pode ser via software (mais comum) ou hardware.
- Impede que utilizadores externos ative os serviços disponibilizados na rede interna.
- Cada vez mais utilizada nos computadores pessoais com ligação permanente à internet.

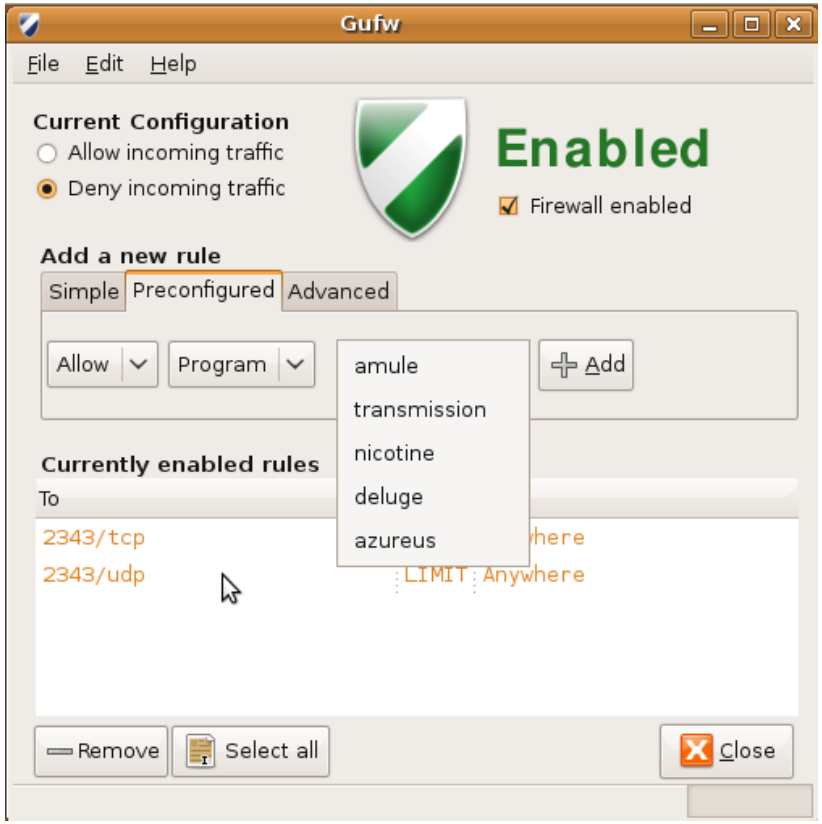


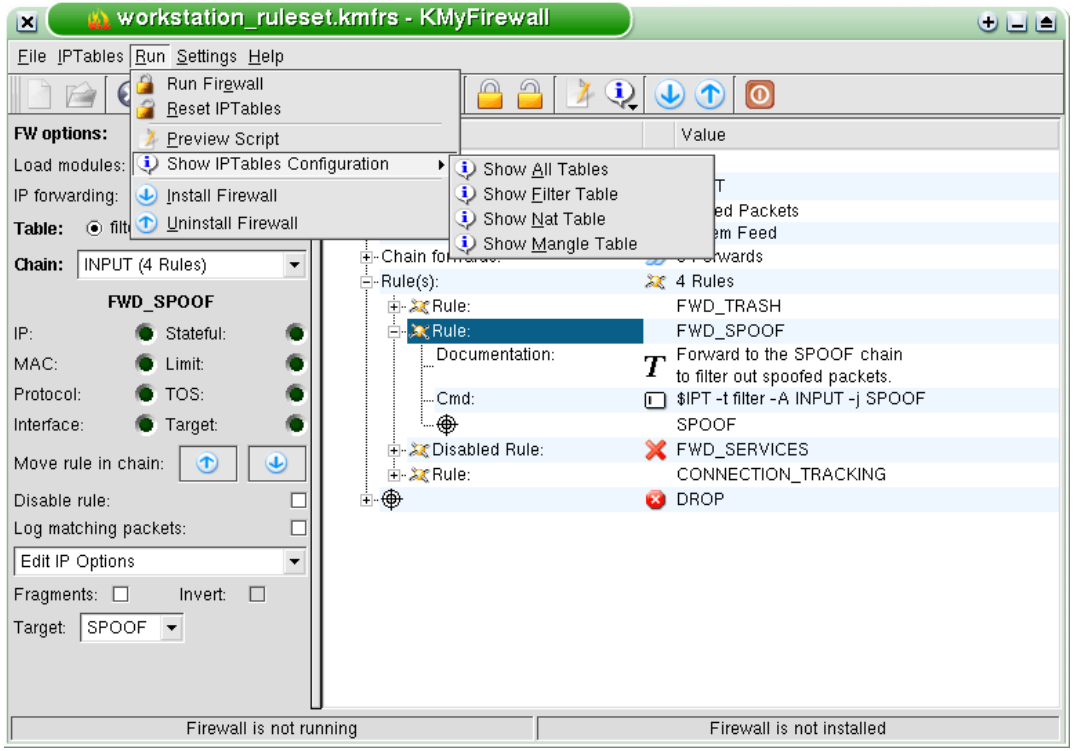
Firewall (hardware)



Firewall (software)

Firewall (software)





Antivírus

- Softwares que procuram detectar, anular ou remover os vírus de computador.
- Uma das grandes riscos de contaminação atuais é a utilização da Internet e de e-mails.
- Um vírus é ativado na maioria das vezes pela ação do usuário executando um arquivo infectado recebido como anexo de um e-mail ou clicando em um link em uma página Internet que contém um código malicioso.
- Grande parte dos problemas está relacionado ao conteúdo da mensagem, que normalmente abusam das técnicas de engenharia social.

Exemplos de Antivírus

Spywares

- Programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador.
- Isto não significa que eles sejam em sua totalidade programas maus. Existem sim, muitos spywares de má índole, criados para coletar informações pessoais e, com elas, praticar atividades ilegais.
- Entretanto, nem todos são assim. Por exemplo: existem empresas de anúncio que se utilizam de spywares para, de forma legal, coletar informações de seus assinantes, com vistas a selecionar o tipo de anúncio que irão lhes apresentar.

Spywares

- Já que nem todos os spywares são maus, você pode se perguntar: “como vou poder saber se um spyware é bom ou mau?”.
- O fato é que não existe um filtro, ou seja, um modo de saber qual spyware é bom e qual é mau.
- O critério que você deve adotar para se proteger é SEMPRE DESCONFIAR.
- Um spyware não-prejudicial só será instalado mediante a autorização do usuário.
- Um spyware maligno, porém, irá se instalar sem que o usuário perceba.

Spywares

- Para evitar esse tipo de ameaça, existem os programas anti-spyware, que possuem bancos de dados completos e constantemente atualizados.
- A partir da comparação de faixas de código entre os spywares conhecidos e os aplicativos do seu computador, será possível detectar se seu computador está ou não sendo espionado.

Hackers, Crackers e Lammers

Aficionado por Informática, profundo conhecedor de linguagens de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros computadores.

Hacker

- Utiliza seu conhecimento para testar recursos de segurança instalados na empresa

Cracker

- Utiliza seu conhecimento para invadir computadores e roubar informações confidenciais.

Lammers

- Não possui grande conhecimento em Informática, são amadores que se passam por hackers ou crackers.
- Tentam buscar falhas e explorar vulnerabilidades usando tutoriais encontrados na Internet.

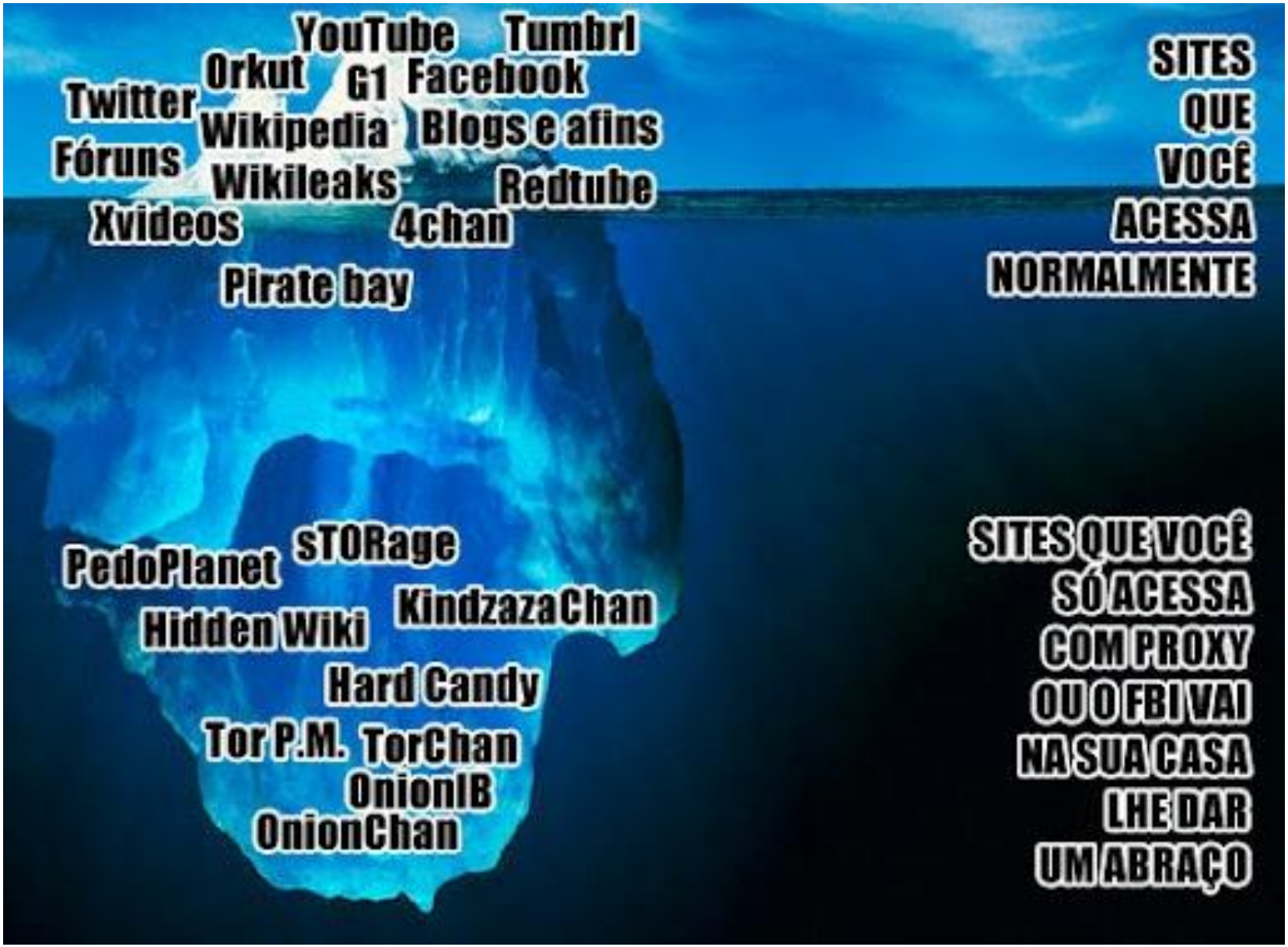
Deep Web – A Internet invisível

- Designação para os sites web que não são indexados em mecanismos de busca padrão.
- A não indexação é devido à natureza dinâmica das páginas. Elas não existem, até que se faça uma requisição, e então a página é dinamicamente criada.
- Pode ser utilizada para as mais diversas ações, geralmente algo que não se queira que seja descoberto.
  - WikiLeaks, Anonymous
  - Livros censurados do passado e da atualidade
  - Venda de órgãos, pedofilia, tráfico de pessoas ..... (**Dark Web**)
  - E muito mais...

Deep Web – A Internet invisível

- TOR (The Onion Route): os dados são passados em vários computadores aleatórios até chegar ao destino.
- Os sites geralmente possuem o domínio .onion e são impossíveis de se soletrar.
  - Wikileaks: http:// kpvz7ki2v5agwt35.onion
  - The Tor Library: http://am4wuhz3zifexz5u.onion
- Na Internet convencional, as informações são mantidas de maneira aberta. No TOR, os dados trafegam criptografados.
- Navegador TOR: conecta a uma rede de proxys anônimos com acesso a Onion. A conexão fica lenta, mas é por que ele utiliza proxy, que deixa seu IP camuflado, deixando-o anônimo na Internet.

Deep Web – A Internet invisível



Política de Segurança Humana

- As pessoas são consideradas o elo mais fraco da segurança da informação.
- A maioria das invasões de sistemas utilizam o fator humano para obter sucesso.
- Engenharia Social:
  - Técnica de influenciar pessoas pelo poder da persuasão. Essa influência tem como objetivo conseguir que as pessoas façam alguma coisa ou forneçam determinada informação a pedido de alguém não autorizado.
- Deve-se estabelecer uma política de segurança detalhada nas empresas, visando conscientizar o usuário dos riscos e ameaças à organização.