Segurança de Redes de Computadores

Ricardo José Cabeça de Souza

www.ricardojcsouza.com.br

ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **OBJETIVOS DA SEGURANÇA**
  - Proteger as informações que trafegam pela rede
  - Busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo oi organização
  - Necessidade de proteção dos dados, contra:
    - A leitura, escrita ou qualquer tipo de manipulação, intencional ou não, confidencial ou não
    - Utilização não autorizada do computador e seus periféricos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **PRINCÍPIOS SEGURANÇA**
  - Confiabilidade
  - Autenticidade
  - Integridade
  - Disponibilidade
  - Não repúdio

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **CONFIABILIDADE**
  - Proteger informações contra sua revelação para alguém não autorizado - interna ou externamente
  - Proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação
  - A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital
  - Cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo
  - No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **AUTENTICIDADE**
  - Está associado com identificação correta de um usuário ou computador
  - O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo
  - É implementado a partir de um mecanismo de senhas ou de assinatura digital
  - Necessária de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema
  - É a medida de proteção de um serviço/informação contra a personificação por intrusos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **INTEGRIDADE**
  - Consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação
  - A modificação inclui ações como:
    - Escrita, alteração de conteúdo, alteração de status, remoção e criação de informações
  - Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro
    - Significa que aos dados originais nada foi acrescentado, retirado ou modificado
  - A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade)

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **DISPONIBILIDADE**
  - Consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização
  - Assegura ao usuário o acesso aos dados sempre que deles precisar
  - Pode ser chamado também de continuidade dos serviços

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **NÃO-REPÚDIO**
  - Impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Correta aplicação desses princípios, a segurança da informação pode trazer benefícios como:**
  - Aumentar a produtividade dos usuários através de um ambiente mais organizado
  - Maior controle sobre os recursos de informática
  - Garantir a funcionalidade das aplicações críticas da empresa

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Incidente de Segurança**
  - Qualquer atividade relativa a rede com implicações negativas de segurança
  - A atividade violou de forma explícita ou implícita a política de segurança

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Incidente de Segurança**
  - Exemplos de incidentes de segurança
    - Tentativas de ganhar acesso não autorizado a sistemas ou dados
    - Ataques de negação de serviço
    - Uso ou acesso não autorizado a um sistema
    - Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema
    - Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Fontes de Incidentes**
  - É muito difícil caracterizar quem realmente causou o incidente
  - Pode ser um adolescente curioso, um estudante universitário, uma pessoa tentando ganhar algo através do ataque ou mesmo um espião procurando informações privilegiadas em seu sistema

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Abrangência da Segurança**
  - Entender a motivação dos ataques
  - Entender a natureza dos ataques
  - Conhecer os mecanismos de defesa
  - Obter uma visão abrangente para definição da melhor estratégia de segurança
  - Envolve diferentes aspectos:
    - Tecnologia
    - Pessoas
    - Negócios
    - Leis

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Possíveis Motivos da Invasão**
  - Utilizar seu computador em alguma atividade ilícita, para esconder sua real identidade e localização
  - Utilizar seu computador para lançar ataques contra outros computadores
  - Utilizar seu disco rígido como repositório de dados
  - Meramente destruir informações (vandalismo)
  - Disseminar mensagens alarmantes e falsas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Possíveis Motivos da Invasão**
  - Ler e enviar *e-mails* em seu nome
  - Propagar vírus de computador
  - Furtar números de cartões de crédito e senhas bancárias
  - Furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você
  - Furtar dados do seu computador, como por exemplo informações do seu Imposto de Renda

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Política de Segurança**
  - Atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados
  - Define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham
  - Deve prever o que pode ou não ser feito na rede da instituição e o que será considerado inaceitável
  - Todo descumprimento à política de segurança é considerado um incidente de segurança
  - Também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a política

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Registro de Eventos (logs)**
  - São registros de atividades gerados por programas de computador
  - No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por sistemas de detecção de intrusão

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **FIREWALL**
  - São dispositivos constituídos pela combinação de *software* e *hardware*, utilizados para dividir e controlar o acesso entre redes de computadores
  - O ***firewall* pessoal** é um *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet, e constitui um tipo específico de *firewall*

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Sistema de Detecção de Intrusão (IDS – *Intrusion Detection System*)**
  - É um programa, ou um conjunto de programas, cuja função é detectar atividades incorretas, maliciosas ou anômalas
  - IDSs podem ser instalados de modo a monitorar as atividades relativas a um computador ou a uma rede

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Falso Positivo**
  - Termo “falso positivo” ´e utilizado para designar uma situação em que um firewall ou IDS aponta uma atividade como sendo um ataque, quando na verdade esta atividade não é um ataque

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

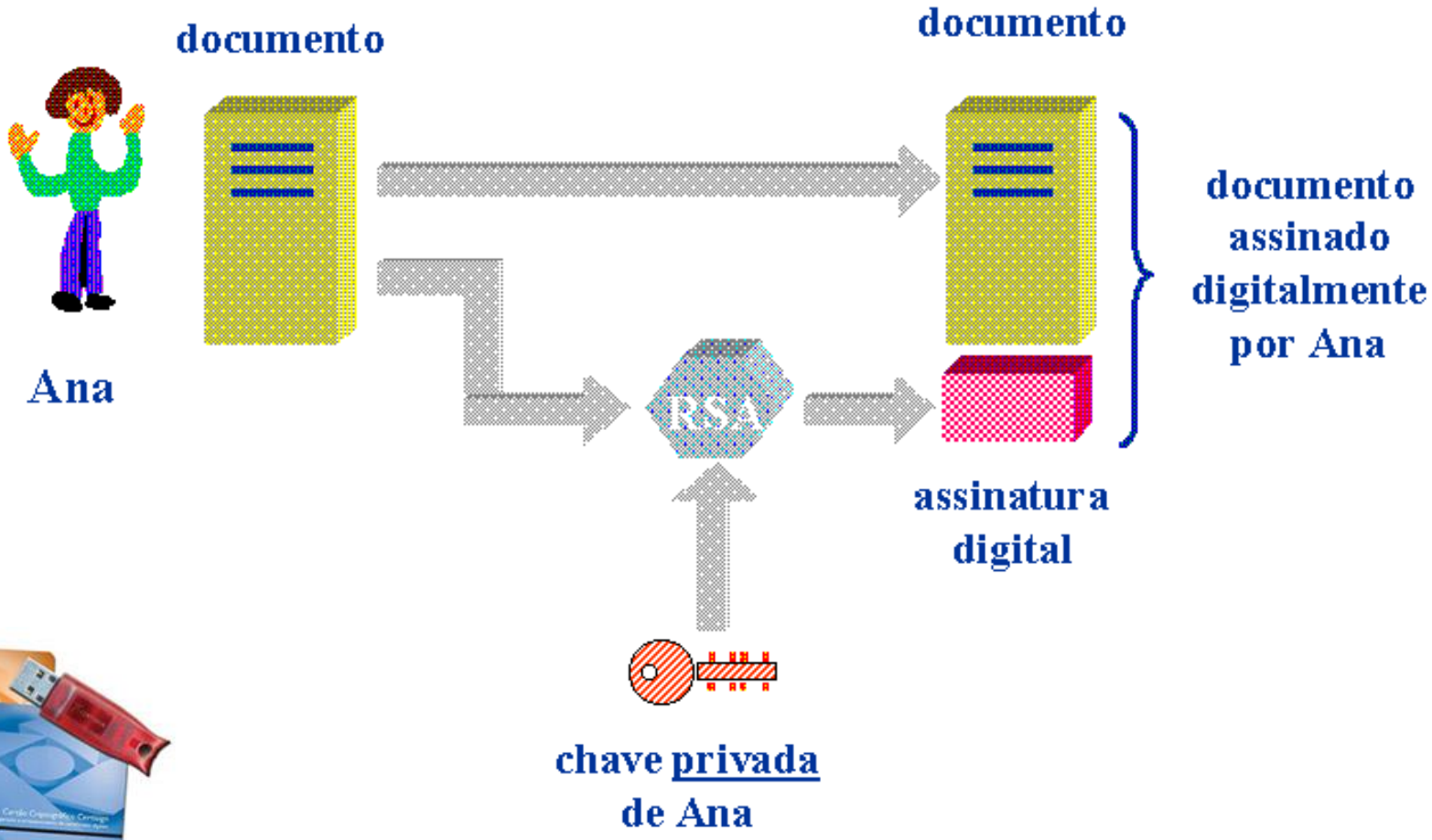
- **Certificado Digital**
  - É um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade
  - O objetivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Certificado Digital**



Fonte: http://www.pontoxp.com/wp-content/uploads/2010/12/CERTIFICADO-DIGITAL-GRATUITO.jpg

Fonte da Imagem: http://www.training.com.br/lpmaia/pub_seg_cripto04.gif

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

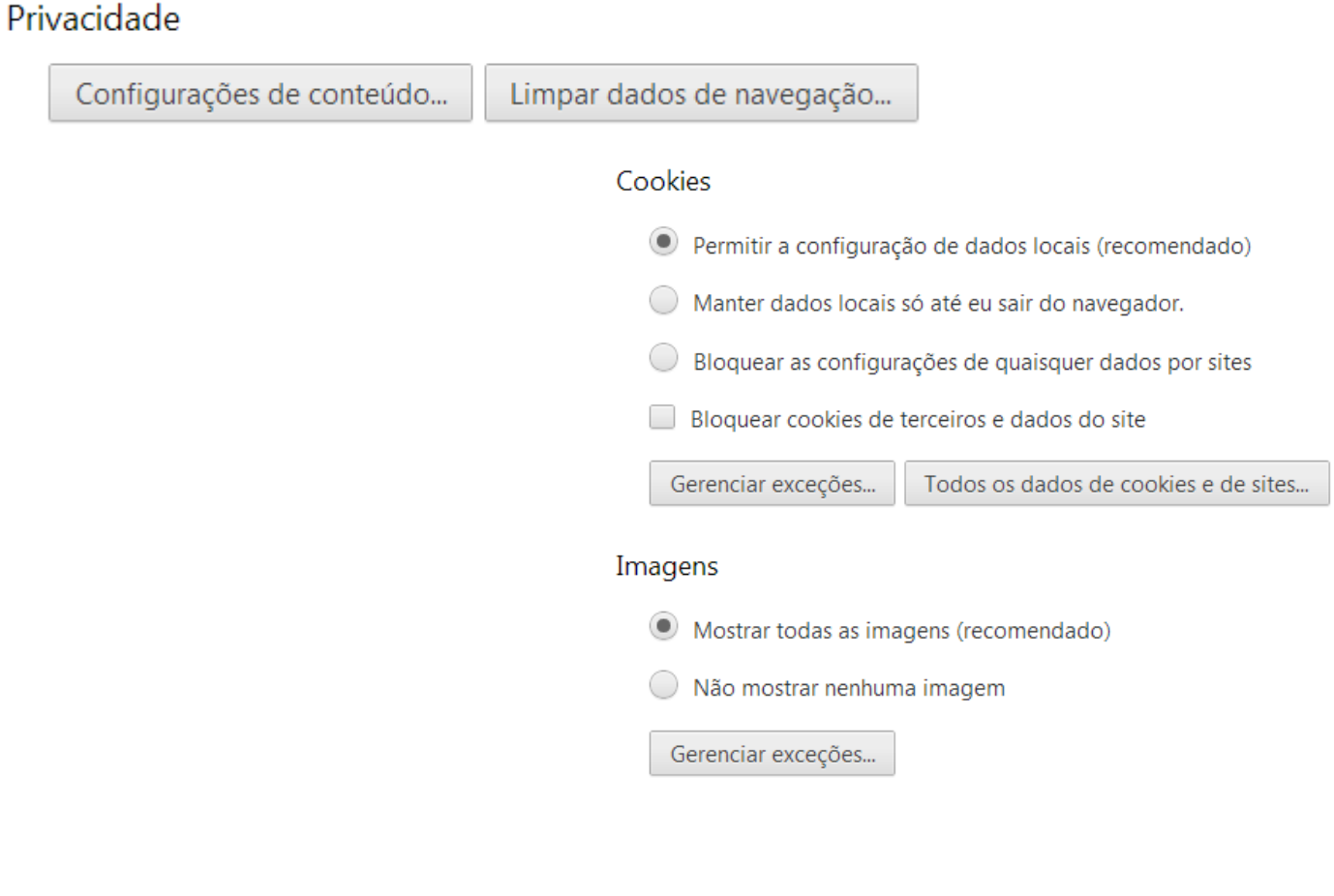
- **Cookies**
  - É um grupo de dados trocados entre o navegador e o servidor de páginas, colocado num arquivo de texto criado no computador do usuário
  - Sua função principal é a de manter a persistência de sessões HTTP
  - São informações guardadas no computador no momento em que o usuário se autentica
  - Essas informações podem ser utilizadas pelos sites de diversas formas, tais como:
    - Guardar a sua identificação e senha quando você vai de uma página para outra
    - Manter listas de compras ou listas de produtos preferidos em sites de comércio eletrônico
    - Personalizar sites pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas
    - Manter a lista das páginas vistas em um site, para estatística ou para retirar as páginas que você não tem interesse dos links

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Cookies (Chrome)**

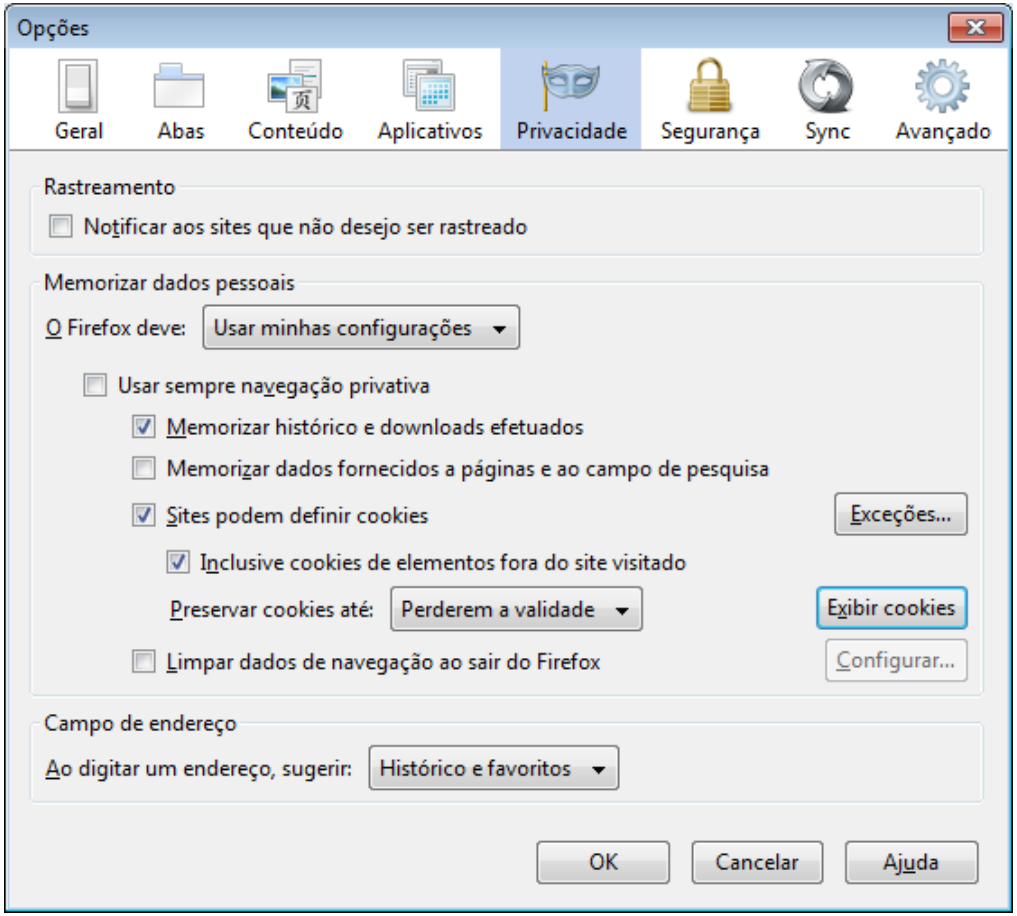


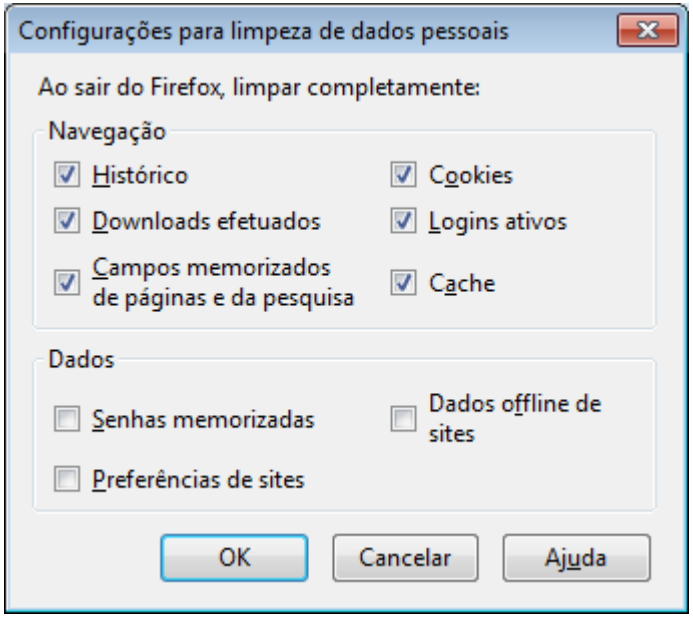
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Cookies (Firefox)**



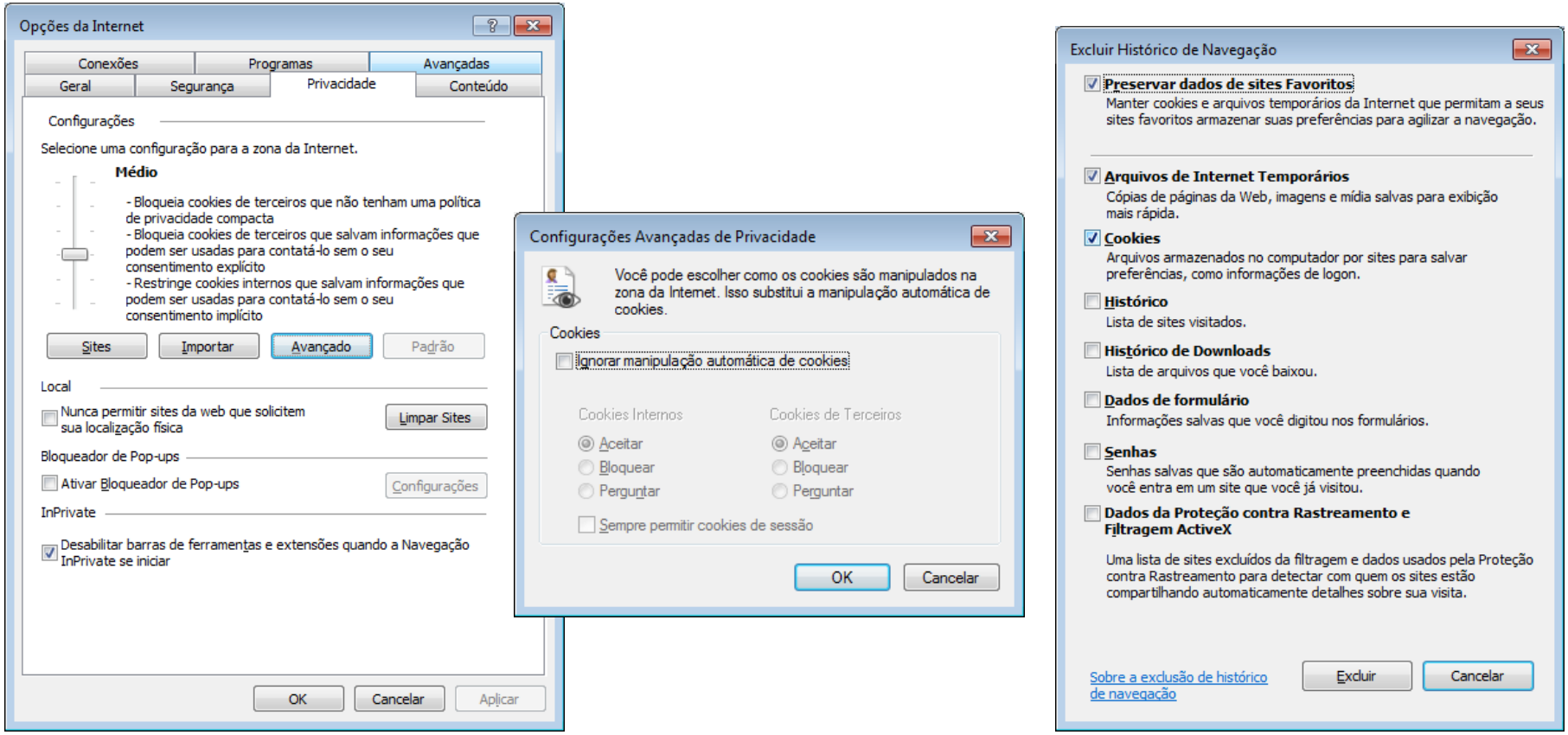


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Cookies (IE)**



www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Engenharia Social**
  - Termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

----- Original Message ----- **From:** Eu & Voce !!!
To: b-21@uol.com.br
Sent: Tuesday, August 09, 2005 10:31 PM
Subject: Minhas Lembranças !!!

Ter você em meus pensamentos e sonhos...viver com você momentos que só existem em mim...
Detalhar em minha mente o calor do seu corpo,o toque de sua pele,o carinho de teu beijo...sem nunca tê-los...
Inventar motivos para tocar seus cabelos e imaginar assim minhas mãos entrelaçadas a eles, trazendo lentamente seus lábios para os meus...
Explode como todo amor, com o mesmo frio na espinha, porém solitário...já nasce agonizante, predestinado a morte súbita. Simples assim...
É como admirar uma bela escultura e não poder tocá-la.
Amor não correspondido...A felicidade em seu início...a desilusão em seu meio...a grande tristeza em seu fim....

Só quero q você entenda com essas poucas palavras q meu amor e muito grande por você....
Te Amo!!! Te Adoro!!! Te Quero!!!
preparei + uma surpresa para você preparei um book de fotos, telefone....
espero q você goste!!!!!!!!!!!!!!!!!!!
se possível queria q assim q você terminasse de ver mim ligasse pra mim ouvir sua linda voz e dizer o q achou BeIjOs.....
book de fotos!

http://galeon.com/kissgreentings/Book.exe

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

Segurança da Informação

----- Original Message ----- **From:** "veja.as.fotos."@mail.amazon.com.br

To: rsp

Sent: Tuesday, June 29, 2004 7:59 PM

Subject: voce esta sendo traido !

sou um amigo seu esse é um aviso

Você esta sendo traído, não tive coragem de te falar mas como imagens falam mais que palavras faça o download das fotos e veja com os seus próprios olhos

VEJA AS FOTOS

Foi a única maneira que encontrei para te avisar

http://amigoeaquele.vila.bol.com.br/fotos.zip

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

----- Original Message ----- **From:** embratel.com.br **To:** suporte@embratel.com.br **Sent:** Friday, August 05, 2005 7:12 AM**Subject:** Comunicado Embratel !!

COMUNICADO DE COBRANÇA

Prezado(a) Cliente,

Este comunicado contém dados pessoais. Para sua segurança é necessário que digite o "Código Verificador" que aparece na imagem abaixo:

Por favor, repita os caracteres ao lado:

Entrar

Se você não conseguir visualizar a imagem clique aqui.

http://glsplanet.terra.com.br/pessoal/marcar/Embratel.scr

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

Segurança da Informação

- **De:** "elvis lei" <elvislei_sup3r@hotmail.com>
  Para: dtic@ifpa.edu.br, mauricioaldenor@ifpa.edu.br, edefreitas@bol.com.br, edijonas@hotmail.com, educonpa@hotmail.com
  Enviadas: Quinta-feira, 9 de Dezembro de 2010 11:06:43

  11:06:44
  1 anexo(s) | Baixar anexo (45,7 KB) Imagem.jpg (45,7 KB)

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

---------- Mensagem encaminhada ----------
De: **SERVICE CONFIMATION** <dany.charoze@orange.fr>
Data: 9 de março de 2012 07:25
Assunto: Re: RE: Fwd: Fw:Fwd: Não entregue o Windows Mail
Para: URGENTE.DE-SERVICO.DE.LOTERIA@btinternet.net
Cher-Membros (e)
Devido ao congestionamento em todas as contas usuários do Yahoo, Hotmail, Gmail, ORANGE,
Box Darty,wanadoo, la poste.
Por razões de segurança da conta de serviço esmaltes parar todas as contas não utilizadas. Para evitar desativação de sua conta, você deve confirmar seu e-mail completo sobre suas informações de login abaixo, clicando no botão responder. O
as informações pessoais solicitadas é para a segurança sua conta Yahoo, Hotmail, Gmail, ORANGE, Box Darty, wanadoo, la poste.
Por favor, deixe todas as informações solicitadas.
Confirmar a sua identidade. VERIFY sua conta agora!

nomeUsuário :..... endereço E-mail :.....
senha :..... .....Ocupação :.....

telefone :.....País de residência:.....
sua conta não será interrompida e continuará como normal. Obrigado pela sua colaboração habitual.
Pedimos desculpas por qualquer desvantagem.
Serviço de Attentivement ao Cliente Conta
Número de casos: 8941624Propriété: Conta da Segurança

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

Segurança da Informação

- **Vulnerabilidade**
  - Definida como uma falha no projeto ou implementação de um *software* ou sistema operacional, que quando explorada por um atacante resulta na violação da segurança de um computador

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Vírus**
  - É um programa capaz de infectar outros programas e arquivos de um computador
  - Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que quando executado também executa o vírus, dando continuidade ao processo de infecção
  - São programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador
  - Têm comportamento semelhante ao do vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam esconder-se para não serem exterminados

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Tipos de Vírus**
  - Existem atualmente várias categorias de vírus de computador
  - Cada categoria com suas características específicas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Vírus de ARQUIVO**
  - Vírus que anexa ou associa seu código a um arquivo
  - Em geral adiciona o código a um arquivo de programa normal ou sobrescreve o arquivo
  - Costuma infectar arquivos executáveis do Windows, especialmente .com e .exe, e não age diretamente sobre arquivos de dados
  - Para que seu poder destrutivo tenha efeito, é necessário que os arquivos contaminados sejam executados

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **Vírus ALARME FALSO**
  - Não causa dano real ao computador, mas consome tempo de conexão à Internet ao levar o usuário a enviar o alarme para o maior número de pessoas possível
  - Se enquadra na categoria de vírus-boato e cartas-corrente

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **BACKDOOR**
  - Como o próprio nome diz, é um vírus que permitem que hackers controlem o micro infectado pela "porta de trás“
  - Normalmente vêm embutidos em arquivos recebidos por e-mail ou baixados da rede
  - Consiste na adição de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente incluindo recursos que permitam acesso remoto (através da Internet)
  - Ao executar o arquivo, o usuário libera o vírus, que abre uma porta da máquina para que o autor do programa passe a controlar a máquina de modo completo ou restrito

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **BOOT**
  - Se infecta na área de inicialização dos disquetes e de discos rígidos
  - Essa área é onde se encontram arquivos essenciais ao sistema
  - Os vírus de boot costumam ter alto poder de destruição, impedindo, inclusive, que o usuário entre no micro

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

- **CAVALO DE TRÓIA (TROJAN)**
  - São programas aparentemente inofensivos que trazem embutidos um outro programa (o vírus) maligno
  - Além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **ENCRIPTADOS**
  - Tipo recente que, por estarem codificados, dificultam a ação dos antivírus

- **MULTIPARTITE**
  - Vírus que infecta registro mestre de inicialização, trilhas de boot e arquivos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **MACRO**
  - Tipo de vírus que infecta as macros (códigos executáveis utilizados em processadores de texto e planilhas de cálculo para automatizar tarefas) de documentos, desabilitando funções como Salvar, Fechar e Sair
- **PROGRAMA**
  - Infectam somente arquivos executáveis, impedindo, muitas vezes, que o usuário ligue o micro

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **MUTANTE**
  - Vírus programado para dificultar a detecção por antivírus
  - Ele se altera a cada execução do arquivo contaminado
- **POLIMÓRFICO**
  - Variação mais inteligente do vírus mutante
  - Ele tenta dificultar a ação dos antivírus ao mudar sua estrutura interna ou suas técnicas de codificação

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **SCRIPT**
  - Vírus programado para executar comandos sem a interação do usuário
  - Há duas categorias de vírus script: a VB, baseada na linguagem de programação, e a JS, baseada em JavaScript
  - O vírus script pode vir embutido em imagens e em arquivos com extensões estranhas, como .vbs .doc, vbs.xls ou js .jpg

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **STEALTH**
  - Vírus "invisível" que usa uma ou mais técnicas para evitar detecção
  - O stealth pode redirecionar indicadores do sistema de modo a infectar um arquivo sem necessariamente alterar o arquivo infectado

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

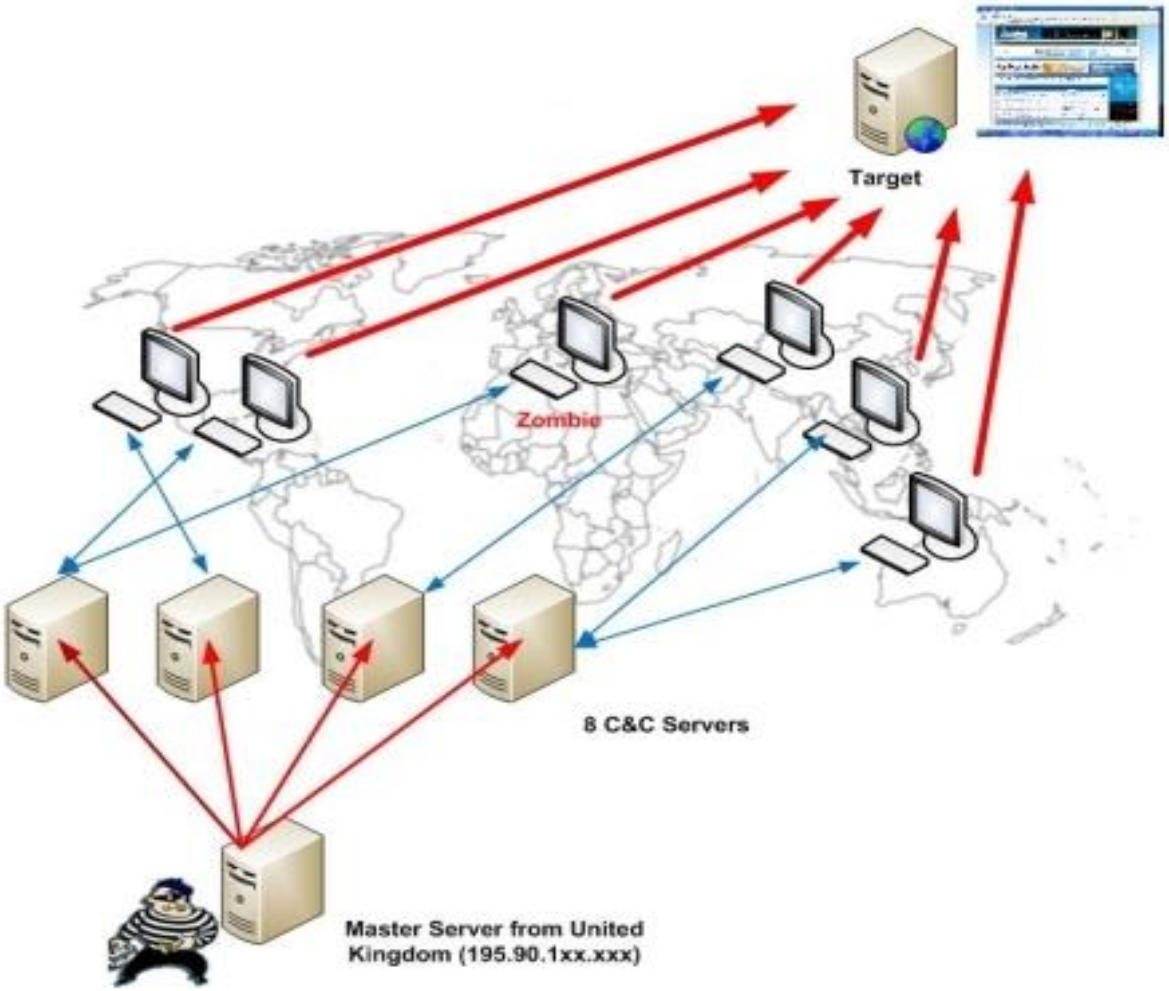
- **BOTNET**
  - O termo *bot* é a abreviação de robot
  - Os criminosos distribuem um software mal-intencionado (também conhecido como malware) que pode transformar seu computador em um bot (também conhecido como zumbi)
  - Quando isso ocorre, o computador pode executar tarefas automatizadas via Internet sem que você saiba

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

Segurança da Informação

- **BOTNET**



Fonte da Imagem: http://4.bp.blogspot.com/-rcwbno8EIq0/TfdoE5ULyHI/AAAAAAAAAZo/SzEV3Z5HGIE/s1600/Master-Control-Server-for-Mydoom-DDoS-Botnet-Tracked-to-UK-3.jpg

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

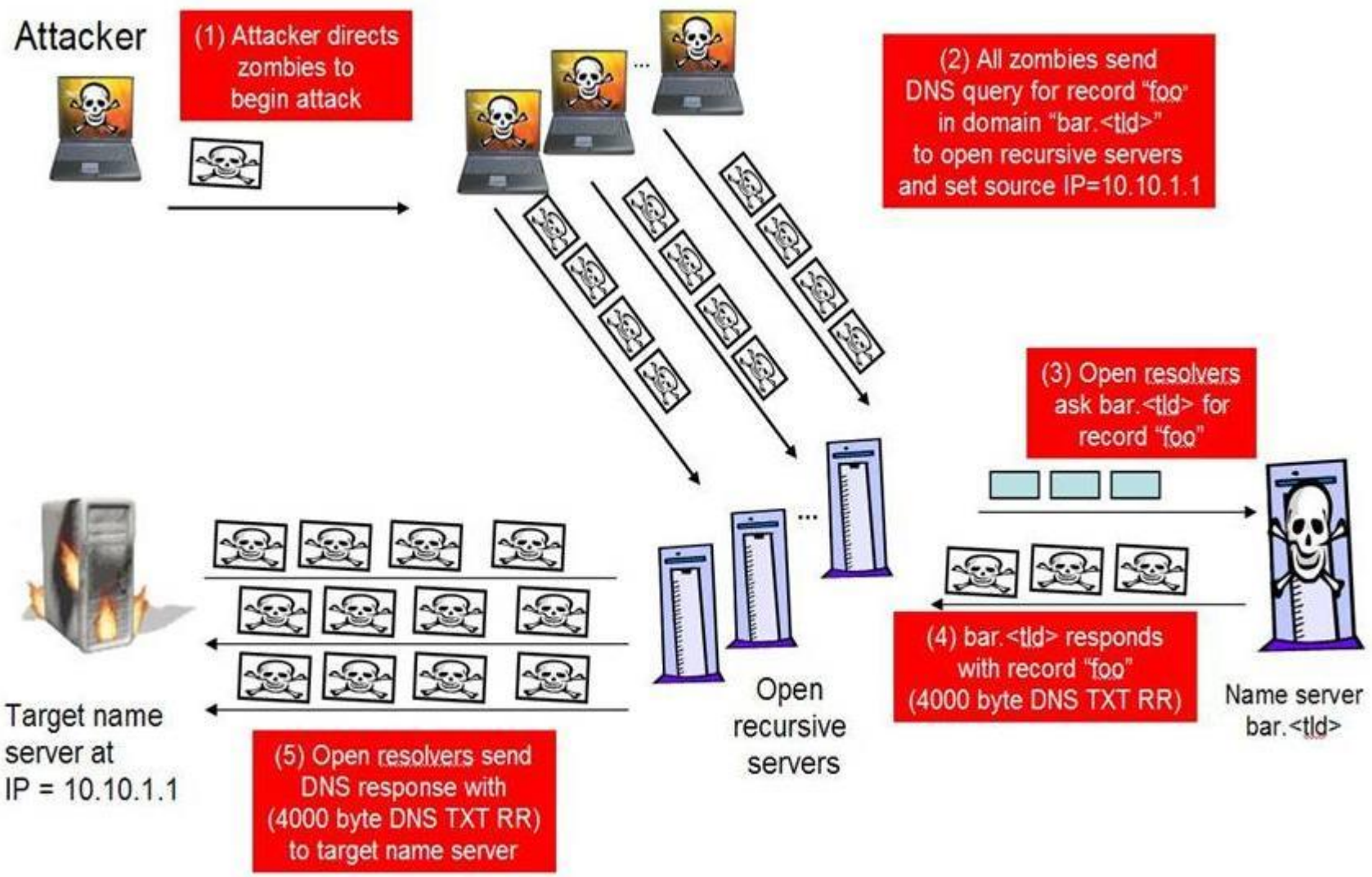
Segurança da Informação

- **BOTNET**
  - Criminosos usam botnets para enviar mensagens de spam, disseminar vírus, atacar computadores e servidores e cometer outros tipos de crimes e fraudes
  - Sintomas:
    - Computador estiver anormalmente lento, travar ou parar de responder com frequência

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação



Fonte da Imagem: http://www.corecom.com/external/livesecurity/dnsfig1.jpg

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Worm**
  - É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador
  - Diferente do vírus, o worm não necessita ser explicitamente executado para se propagar
  - Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores
  - São notadamente responsáveis por consumir muitos recursos

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Segurança da Informação

- **Negação de Serviço (Denial of Service)**
  - Ataques onde o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet
  - Exemplos:
    - Gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo
    - Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível
    - Tirar serviço importantes de um provedor do ar, impossibilitando o acesso dos usuários às suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

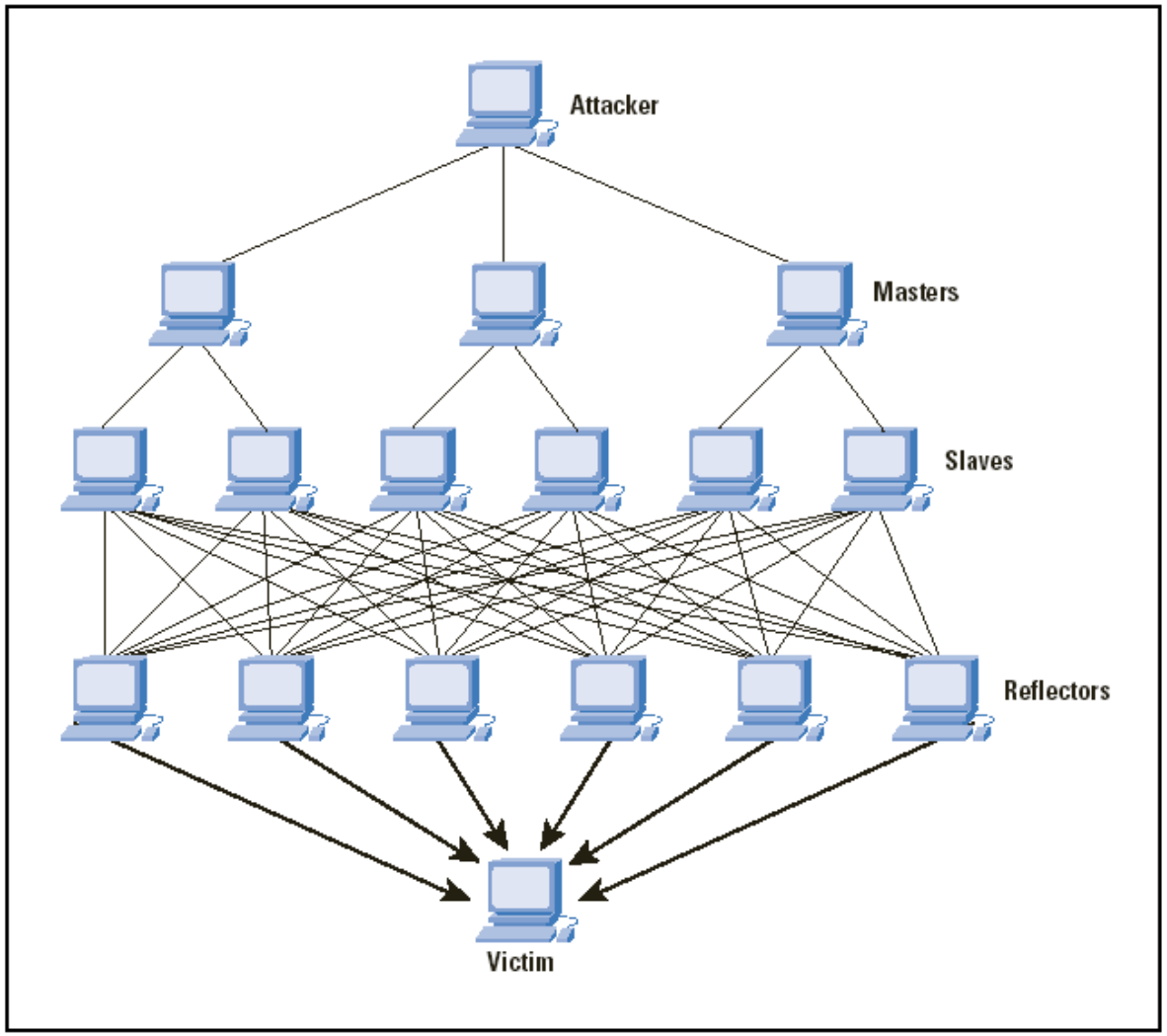
- **DDoS (Distributed Denial of Service)**
  - Constitui um ataque de negação de serviço distribuído
  - Um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Segurança da Informação

Figure 5: A DRDoS Attack



Fonte da Imagem: http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_7-4/dos_figure_5.gif

Referências

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- Lima, Marcelo. Nakamura, Emílio. **Segurança de Redes e Sistemas**. Versão 1.1.0. Escola Superior de Redes RNP:2007.
- MEDEIROS, Carlos Diego Russo. **SEGURANÇA DA INFORMAÇÃO: Implantação de Medidas e Ferramentas de Segurança da Informação**. Universidade da Região de Joinville – UNIVILLE, 2001.
- NIC BR Security Office. **Cartilha de Segurança para Internet. Parte VII: Incidentes de Segurança e Uso Abusivo da Rede**. Versão 2.0, 2003.
- NIC BR Security Office. **Cartilha de Segurança para Internet. Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção**. Versão 2.0, 2003.
- FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.