
egi
Escola de Governança
da Internet no Brasil

# Fundamentos de Segurança da Informação

Cristine Hoepers, D.Sc.
Klaus Steding-Jessen, D.Sc.

12/08/2014 – 14:00 às 15:30h

# Objetivos

**Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência**

De forma não exaustiva

**Subsidiar os participantes para as crescentes discussões sobre privacidade, segurança, estabilidade e resiliência nos fóruns nacionais e internacionais de governança da Internet**

Embasamento técnico para identificar e questionar falácias, mitos e artigos não embasados

# Agenda

- **Motivações**
- **Modelo de Segurança da Informação**
- **Riscos, ameaças e ataques**
- **Medidas de Segurança**
- **Implementando Segurança e Resiliência**
  - **Conceitos e atores envolvidos**
- **Considerações finais**

# Motivações

# WSIS:
# Declaration of Principles

**Document WSIS-03/GENEVA/DOC/4-E**

**12 December 2003**

**[...]**

**B5) Building confidence and security in the use of ICTs**

**35.** Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

**[...]**

http://www.itu.int/wsis/docs/geneva/official/dop.html

# CGI.br:
# Princípios para a Governança e Uso da Internet no Brasil

**CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL**

**Fevereiro de 2009**

**[...]**

**8. Funcionalidade, segurança e estabilidade**
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

**[...]**

**http://www.cgi.br/resolucoes/documento/2009/003**

# NETmundial:
# Internet Governance Principles

**NETmundial Multistakeholder Statement**

**April, 24th 2014, 19:31 BRT**

**[...]**

**SECURITY, STABILITY AND RESILIENCE OF THE INTERNET**

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.

**[...]**

http://www.netmundial.org/references/


'The forum was running an outdated version of vBulletin [without] admin panel protection'

'Ubuntu One and Launchpad are not affected by the breach'

Hacker hijacks ISPs, steals $83,000 from Bitcoin mining pools | ZDNet

www.zdnet.com/hacker-hijacks-isps-steals-83000-from-bitcoin-mining

Reader

# Hacker hijacks ISPs, steals $83,000 from Bitcoin mining pools

***Summary:*** *Bitcoin exchanges and trading posts have been hacking targets over the past year, but now one hacker has taken on ISPs to loot Bitcoin from mining pools.*

By Charlie Osborne for Zero Day | August 8, 2014 -- 10:02 GMT (03:02 PDT)

A hijacker was able to use a fake Border Gateway Protocol (BGP) broadcast in order to compromise networks belonging to some of the biggest names in the field -- including Amazon, Digital Ocean, and OVH, among others -- between February and May 2014. According to the researchers, at least 51 networks were compromised from 19 different ISPs, and at least one hijacker was able to use this flaw to redirect cryptocurrency miners' connections to a hijacker-controlled mining pool, therefore collecting the miner's profit for themselves.

RISK A

US restaurant chain P.F. Chang's China Bistro plans to temporarily bring back manual credit card imprinting while it investigates a security breach that allowed hackers to steal customer payment card data from multiple stores.

# P.F. Chang's turns to vintage 1970s tech after credit card breach

Restaurant chain goes old school as it investigates theft from multiple stores.

by **Dan Goodin** - June 13 2014, 1:47pm BRT

HACKING INTERNET CRIME 207

Brasileiros evitam pagar as contas pela internet por medo de fraudes – Meu Bolso – iG

Um levantamento do **iG** com 108 internautas que não pagam as contas pela internet constatou que 72% evitam o acesso online por acreditar ser um ambiente inseguro. Outros 10% responderam que não sabem utilizar o sistema – e 12% justificam que preferem ir ao banco pessoalmente.

HOME | MERCADOS | EMPRESAS | FINANÇAS PESSOAIS | IMPOSTO DE RENDA | COLUNAS | CARREIRAS | SEU NEGÓCIO | MAIS SITES

# Brasileiros evitam pagar as contas pela internet por medo de fraudes

Por **Taís Laporta - iG São Paulo** | 05/08/2014 12:00

Texto | 1 pessoas lendo | 6 Comentários | 9 | Tweetar 38 | Recomendar

## No Brasil, apenas 4 em cada 10 transações bancárias foram feitas pela internet; consumidores abrem mão da comodidade online por julgar o sistema dos bancos inseguro

"Não confio em transações bancárias pela internet". Apreensivo, Thiago Rodrigues, de 25 anos, prefere pagar seus compromissos em caixas eletrônicos ou enfrentar longas filas no banco. Ele desativou o acesso online a todas suas contas e, quando precisa visualizar os extratos, vai pessoalmente a uma agência.

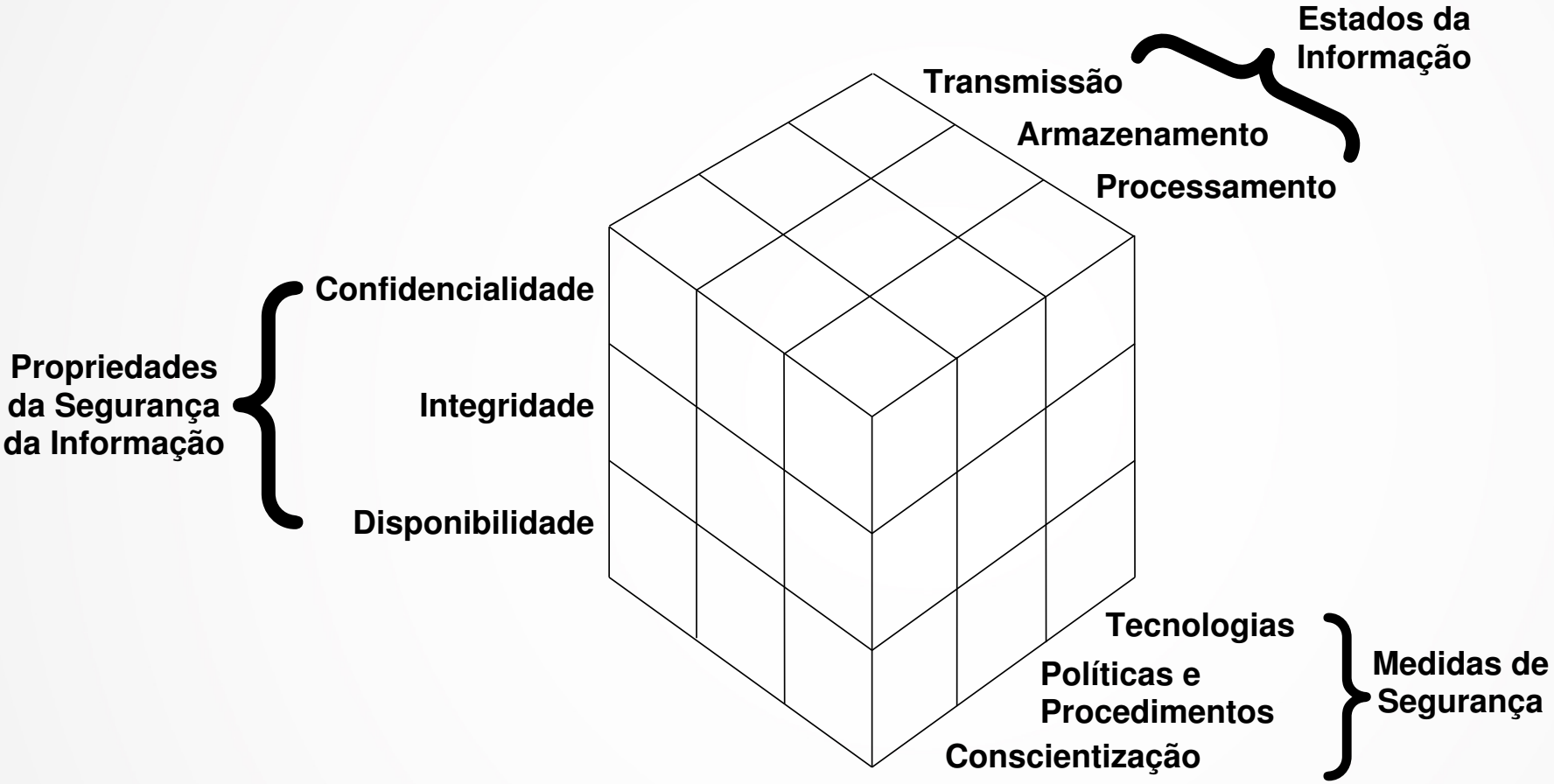
**Leia mais:** Bancos oferecem cartão de crédito para crianças, mas há risco

"Meu pai teve um valor retirado de sua conta e não conseguiu recuperar. Depois descobrimos que ele usou um computador que havia sido hackeado", recorda Thiago, só

# Segurança da Informação

egi

# As informações estão em diversos locais e a segurança depende de múltiplos fatores




***McCumber Information Security Model***
http://www.ibm.com/developerworks/security/library/s-confnotes2/

# Revendo conceitos:
# **Propriedades da Segurança da Informação**

**Confidencialidade –** é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

**Integridade –** é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

**Disponibilidade –** é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

# Exemplos de Quebras das Propriedades da Segurança da Informação

**Confidencialidade –** alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda.

**Integridade –** alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

**Disponibilidade –** o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

# Revendo conceitos:
# **Privacidade vs Confidencialidade**

**Do ponto de vista de Segurança da Informação:**

**Privacidade –** habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.

**Confidencialidade –** envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.

# De Quem Estamos Querendo nos Proteger?

# Revendo conceitos: **Vulnerabilidade e Risco**

**Vulnerabilidade –** Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

**Risco –** é o potencial de que uma dada **ameaça** venha a explorar **vulnerabilidades** em um determinado **ativo**, de modo a comprometer a sua segurança.

# Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**


**Sistemas na Internet**

**Riscos**

**Atacantes**

- criminosos
- espionagem industrial
- governos
- vândalos

**Vulnerabilidades**

- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

# Como Ocorrem os Ataques

# Revendo conceitos:
# **Ataque, *Exploit* e Código Malicioso**

**Ataque –** qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.

**Exploit –** programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador.



**Código Malicioso –** termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel.

- Tipos específicos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

# Revendo conceitos:
# **Tipos de Ataque**

**Engenharia social –** técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações.

**Varredura em redes (*scan*) –** consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados.

**Negação de serviço distribuída (DDoS) –** atividade maliciosa, coordenada e distribuída, pela qual um conjunto de computadores e/ou dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

**Força bruta –** consiste em adivinhar, por tentativa e erro, um nome de usuário e senha de um serviço ou sistema.

**Invasão ou comprometimento –** ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

**Desfiguração de página (*Defacement*) –** consiste em alterar o conteúdo da página *Web* de um *site.*

**Escuta de tráfego –** consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos.

# Cenário:
# **Ataque Contra Usuários de Internet**

Usuário recebe e-mail com um PDF em anexo [Ex.: NFE, Ata de reunião, pedido de cotação, etc]

PDF é aberto usando uma versão vulnerável do leitor (Ex. Acrobat)

PDF tem conteúdo malicioso e explora vulnerabilidade do programa leitor

Código do atacante é executado no computador

Código baixa e executa um *malware*

*Malware* se conecta em um servidor de Comando e Controle

*Malware* recebe comandos do atacante para, por exemplo:

- instalar *spyware* (*keylloger, screenloger*, etc)
- exfiltrar dados
- enviar spam
- atacar outras redes (DDoS, invasões, etc)
- enviar e-mails para todos os contatos do usuário, com um PDF malicioso, para continuar se propagando

# Cenário:
# **Ataque Contra Servidores Web**

Atacante instala ferramentas em um *site* já comprometido

Varre a Internet em busca de *sites* com sistemas CMS (Wordpress, Joomla, etc)

Constrói uma lista de *sites* a serem atacados

Em cada *site* realiza um ataque de força bruta de *logins* e senhas

Ao conseguir acesso ao *site* pode, entre outras coisas:

- alterar o seu conteúdo (*defacement*)
- desferir ataques contra outros sistemas ou redes (como DDoS, enviar *spam*, tentar invadir outros sistemas, etc)
- levantar páginas de *phishing*
- inserir *scripts* maliciosos, que exploram vulnerabilidades dos navegadores dos visitantes do *site*, com o objetivo de infectar os usuários (ataques de *drive-by*)
- instalar suas ferramentas e iniciar a busca por outros *sites* com CMS para reiniciar o ciclo do ataque

# Reflexão:
# **Lei 12.737 – Art. 2º**

**Art. 2º** O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

**Invasão de dispositivo informático**

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou **instalar vulnerabilidades** para obter vantagem ilícita

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

**O que se pretendia tipificar?**

- **a inserção de vulnerabilidades? –** que geralmente é feita pelo desenvolvedor, usuário ou administrador de sistemas, não intencionalmente
- **ou a exploração de vulnerabilidades? –** atividade realizada por um atacante que tenta invadir um sistema

# Medidas de Segurança

# Revendo conceitos:
# **Controle de Acesso e Correlatos**

**Controle de acesso –** garantir que recursos só sejam concedidos àqueles usuários que possuem permissão.

**Identificação –** permitir que uma entidade se identifique, ou seja, diga quem ela é. Ex: conta de usuário, conta do banco, *e-mail*

**Autenticação –** verificar se a entidade é realmente quem ela diz ser. Ex.: senha, *token*, biometria

**Exemplo: Acesso a serviços Web**

- **conta de usuário –** é a identificação
- **senha –** é a autenticação
- ***cookies* –** permitem identificar os acessos que fazem parte de uma mesma sessão

# Revendo conceitos:
# **Criptografia e Correlatos**


**Criptografia –** Ciência e arte de escrever mensagens em forma cifrada ou em código.

> É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

**chave –** similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos.

**certificado digital –** registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. É emitido por uma **autoridade certificadora**.

**assinatura digital –** código usado para comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada.

# Ferramentas de Segurança:
# **Proteção de Dados em Trânsito**

**SSL/TLS, SSH e IPSec –** protocolos que, por meio de criptografia, fornecem confidencialidade e integridade nas comunicações entre um cliente e um servidor.

**VPN –** termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Em geral utilizam criptografia e outros mecanismos de segurança para proteger os dados em trânsito.

- Existem serviços na Internet que dizer fornecer uma VPN, mas que apenas fornecem serviços de *proxy* que "ocultam" o IP de origem – a maior parte destes serviços não cifra o conteúdo em trânsito.

**PGP –** programa que implementa operações de criptografia, como cifrar e decifrar conteúdos e assinatura digital.

- Normalmente utilizado em conjunto com programas de *e-mail*.

# Ferramentas de Segurança: **Registros de Eventos (*Logs*)**

São os registros de atividades gerados por programas e serviços de um computador. A partir da análise destas informações é possível:

- detectar problemas de *hardware* ou nos programas e serviços instalados no computador;
- detectar um ataque;
- detectar o uso indevido do computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema.

## Exemplos – *logs* de sistema:

```
Jul  4 10:47:01 localhost UserEventAgent[11]:
CaptiveNetworkSupport:CreateInterfaceWatchList:2788 WiFi Devices Found. :)
Jul  4 10:47:02 localhost configd[14]: network configuration changed.

Jul 28 15:07:21 notebook Software Update[443]: Can't instantiate
distribution from http://swcdn.apple.com/content/downloads/11/05/041-0925/
g27esO4pw9re5ggrfp3suf8ew6t53asfz8/041-0925.English.dist: Error
Domain=NSXMLParserErrorDomain Code=4 "zero length data"
UserInfo=0x7fed3da20e50 {NSLocalizedDescription=zero length data}

Jul 30 13:00:16 hostname sshd[1243]: Accepted password for usuario from
2001:db8:0:1::6 port 35849 ssh2
```

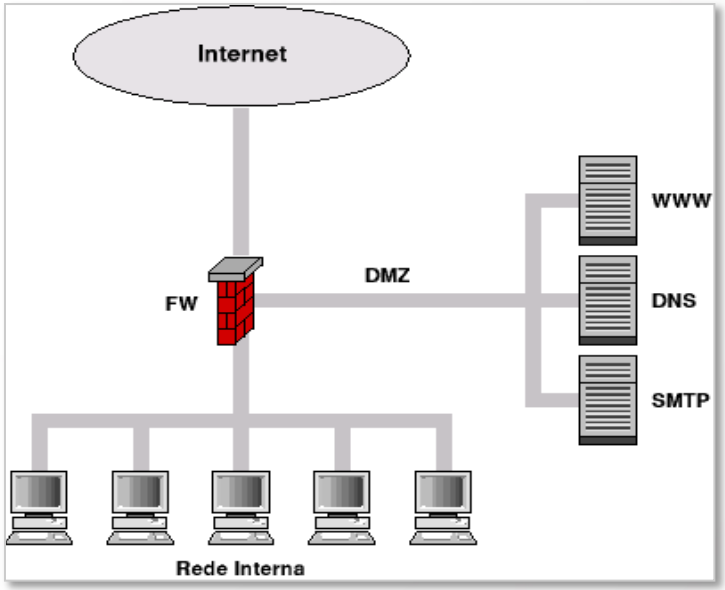
# Ferramentas de Segurança:
# **Proteção Contra Comprometimentos – 1**

***Firewall* –** usado para dividir e controlar o acesso entre redes de computadores.

- um *firewall* só pode atuar no tráfego que passa por ele
- quando o *firewall* é instalado para proteger um computador é chamado de *firewall* pessoal

**Opera com base em regras pré-definidas**

- Mais comum: com base nas informações dos cabeçalhos IP, TCP, UDP, etc
  - consegue bloquear com base em portas e protocolos específicos
  - pode manter "estado"
- *Firewall* de aplicação – nome dado quando a filtragem é feita com base na análise do conteúdo
  - "assinaturas" de ataques



# Ferramentas de Segurança:
# **Proteção Contra Comprometimentos – 2**

## Exemplos de *logs* de *firewall* pessoal:

```
#Software: Microsoft Windows Firewall

2005-04-11 08:05:57 DROP UDP 123.45.678.90 123.456.78.255 137 137 78 - - -
- - - - - RECEIVE

#Software: MacOS X Firewall

Jul 18 16:40:11 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:80 from 118.244.186.157:53031

Jul 18 16:46:22 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:8080 from 118.244.186.157:53031

Jul 18 16:49:30 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:3128 from 118.244.186.157:53031

Jul 18 16:59:09 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:22 from 116.10.191.176:6000

Jul 18 17:16:18 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:3389 from 218.77.79.43:47811

Jul 18 17:19:42 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:22 from 116.10.191.223:6000

Jul 18 17:40:20 notebook Firewall[65]: Stealth Mode connection attempt to
UDP 192.0.2.209:5060 from 199.19.109.76:5079
```

# Ferramentas de Segurança:
# **Proteção Contra Comprometimentos – 3**

***Antimalware* –** procura detectar e, então, anular ou remover os códigos maliciosos de um computador.

- Os programas **antivírus**, ***antispyware***, ***antirootkit*** e ***antitrojan*** são exemplos de ferramentas *antimalware*.


**Filtro *antispam* –** permite separar os *e-mails* conforme regras pré-definidas.

- Pode ser implementado com base em análise de conteúdo ou de origem das mensagens.

# Ferramentas de Segurança:
# **Detecção de Atividades Maliciosas**

**IDS –** programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas

- geralmente implementado com base na análise de *logs* ou de tráfego de rede, em busca de padrões de ataque pré-definidos.

**Fluxos de rede (*Flows*) –** sumarização de tráfego de rede

- armazena IPs, portas e volume de tráfego
- permite identificar anomalias e perfil de uso da rede
- em segurança usado para identificar:
  - ataques de negação de serviço
  - identificar computadores comprometidos

# Implementando Segurança e Resiliência

# Revendo conceitos:
# **Resiliência Operacional**

**Um sistema 100% seguro é muito difícil de atingir**

**Para conseguir uma segurança razoável tem-se tentado atingir os seguintes objetivos:**

- Detectar comprometimentos o mais rápido possível
- Diminuir o impacto
  - Conter, mitigar e recuperar de ataques o mais rápido possível

**Novo paradigma: Resiliência**

- Continuar funcionando mesmo na presença de falhas ou ataques

# Como Obter Resiliência

- **Identificar o que é crítico e precisa ser mais protegido**
- **Definir políticas (de uso aceitável, acesso, segurança, etc)**
- **Treinar profissionais para implementar as estratégias e políticas de segurança**
- **Treinar e conscientizar os usuários sobre os riscos e medidas de segurança necessários**
- **Implantar medidas de segurança que implementem as políticas e estratégias de segurança**
  - como aplicar correções ou instalar ferramentas de segurança
- **Formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes**

# Revendo conceitos:
# **Gestão de Incidentes e Correlatos**

**Incidente de Segurança em Computadores –** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

**Gestão de Incidentes –** definição de políticas e processos que permitam a identificação e o tratamento de incidentes de segurança

**CSIRT –** acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores

Outros acrônimos: IRT, CERT, CIRC, CIRT, SERT, SIRT

**Inserção nas discussões de Governança:**

**IGF Best Practices Forums**

- Establishing and supporting Computer Emergency Response Teams (CERTs) for Internet security
- Regulation and mitigation of unwanted communications (e.g. "spam")

# Papel dos CSIRTs

**A redução do impacto de um incidente é conseqüência:**

- da agilidade de resposta
- da redução no número de vítimas

**O papel do CSIRT é:**

- auxiliar a proteção da infra-estrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas
- auxiliar a detecção de incidentes de segurança
- responder incidentes – retornar o ambiente ao estado de produção

**O sucesso depende da confiabilidade**

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

**O CSIRT não é um investigador**

# Evolução histórica:
# **Tratamento de Incidentes no Brasil**

**Agosto/1996:** o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]

**Junho/1997:** o CGI.br cria o CERT.br (naquele tempo chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]

**Agosto/1997:** a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]

**1999:** outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs

**2002–2004 :** grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal

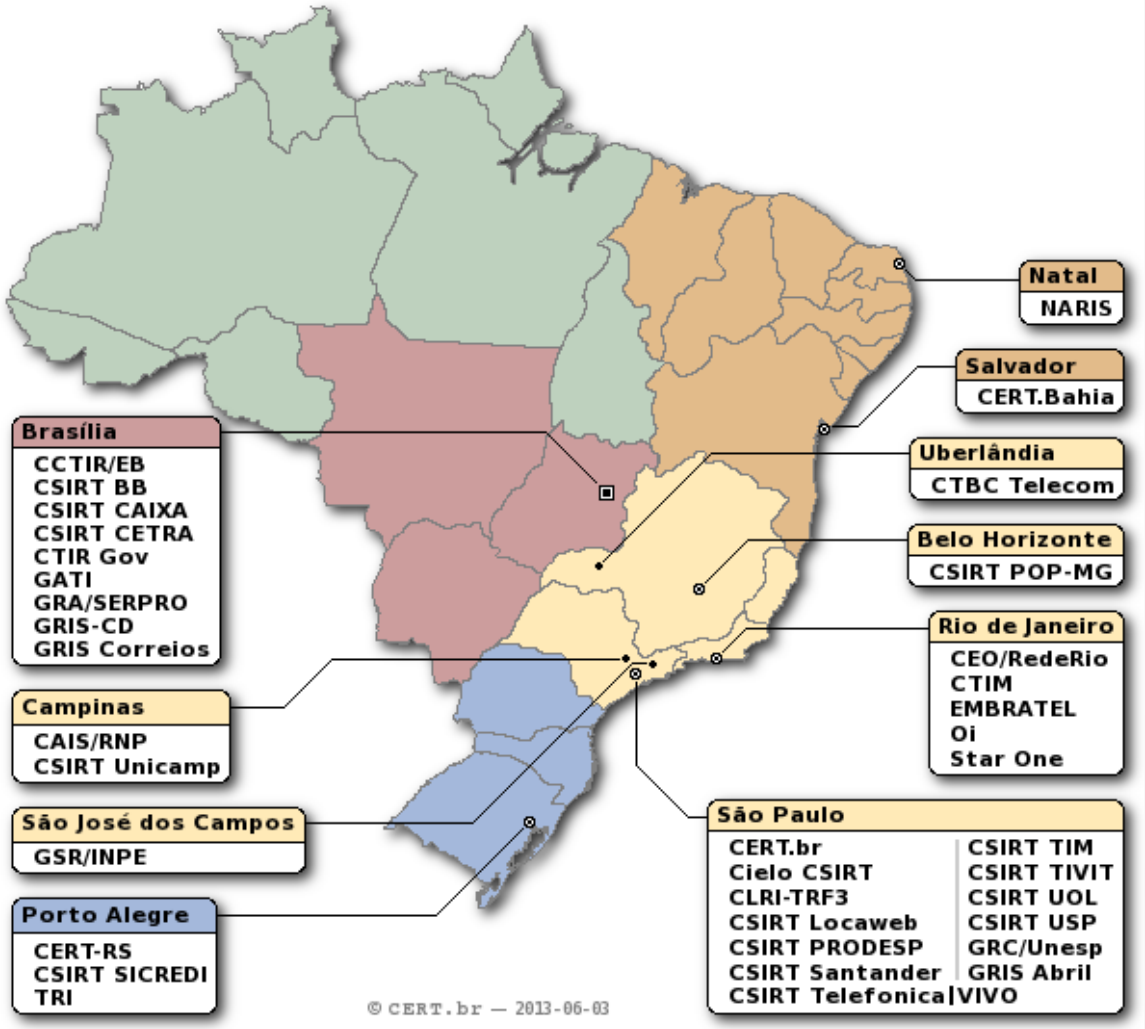
**2004:** o CTIR-Gov foi criado, com a Administração Pública Federal como seu público alvo[5]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/index.php/missao
[5] http://www.ctir.gov.br/sobre-CTIR-gov.html

# Grupos de Tratamento de Incidentes Brasileiros:

## 37 times com serviços anunciados ao público

| Público Alvo | CSIRTs |
|---|---|
| Qualquer Rede no País | CERT.br |
| Governo | CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, GRA/SERPRO, GRIS-CD, CSIRT CETRA, GRIS Correios |
| Setor Financeiro | Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander |
| Telecom/ISP | CTBC Telecom, EMBRATEL, CSIRT Telefonica\|VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, StarOne, Oi, |
| Academia | GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CEO/RedeRio, CERT.Bahia, CSIRT USP, GRC/UNESP, TRI |
| Outros | CSIRT TIVIT, GRIS Abril |




http://www.cert.br/csirts/brasil/

# Considerações Finais

# Questões em aberto:
# **Controle vs Segurança**

**Supostas medidas de segurança, mas usadas para controle, podem gerar reações contra a segurança como um todo**

- uso indiscriminado da biometria em escolas, academias, acesso a edifícios, etc
- RFID (*Radio Frequency Identification*) em carros, cartões de crédito e passaportes

**Quem tem acesso? Com que finalidade?**

**Como estes dados estão protegidos?**

**Seu uso traz mesmo mais segurança no contexto em que estão sendo usados?**

# Questões em aberto:
# **Privacidade *online***

**Um grande risco pode ser não entender a tecnologia**

- As informações que um navegador fornece a um *site*, permitem identificação mais únivoca que um endereço IP válido
- Medidas de segurança não são contra a privacidade, mas sim essenciais para mantê-la

**É necessário que modelos de negócio e regras sejam claros**

- Serviços não são gratuitos, são pagos com informações providas por seus usuários

# Referências:
# Fontes dos Conceitos Apresentados

**Cartilha de Segurança para a Internet**
http://cartilha.cert.br/

***Security Engineering, 2nd Edition, 2008, Ross Anderson***
http://www.cl.cam.ac.uk/~rja14/book.html

***Glossary of Security Terms,* SANS *Institute***
http://www.sans.org/security-resources/glossary-of-terms/

***RFC 2196: Site Security Handbook***
http://tools.ietf.org/html/rfc2196

***Cyber Risk and Resilience Management, CERT/CC***
http://www.cert.org/resilience/

# Obrigado

**Cristine Hoepers, D.Sc.**
**cristine@cert.br**
**Klaus Steding-Jessen, D.Sc.**
**jessen@cert.br**

nic.br cgi.br

www.nic.br | www.cgi.br