nic.br cgi.br | cert.br

Ciclo de Palestras – Segurança na Internet

17 de junho de 2015

Campinas, SP

Protegendo suas Contas de Acesso na Internet

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

Evolução da Internet no Brasil

1989	**Criação e delegação do código de país (ccTLD) ".br" à FAPESP**
1991	**Primeira *conexão TCP/IP brasileira, realizada entre a FAPESP e o Energy Sciences Network* (ESNet) por meio do Fermilab *(Fermi National Accelerator Laboratory)***
1995	**Criação do CGI.br (Portaria Interministerial MC/MCT nº 147, de 31 de maio) com a missão de coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados**
1995	**Criação do Registro.br**
1997	**Criação do CERT.br (à época NBSO)**
2005	**Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil**

http://www.nic.br/imprensa/releases/2010/rl-2010-12.htm

Comitê Gestor da Internet no Brasil – CGI.br

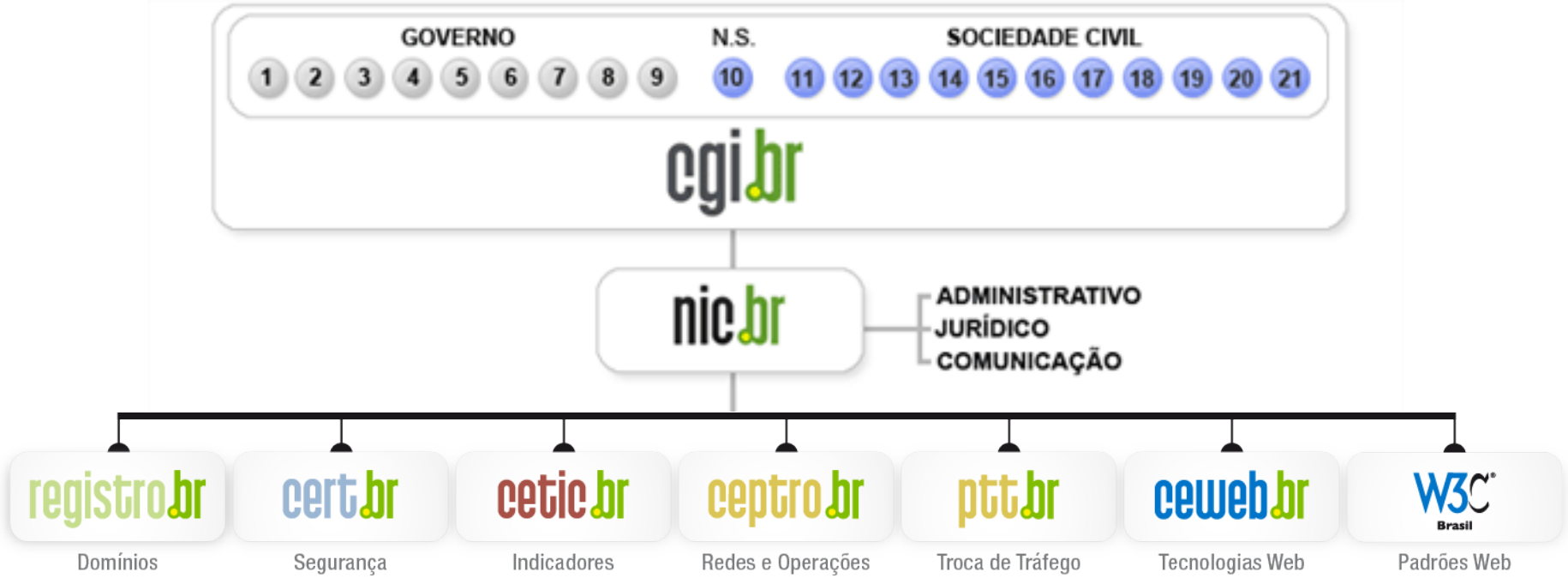
Tem a missão de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

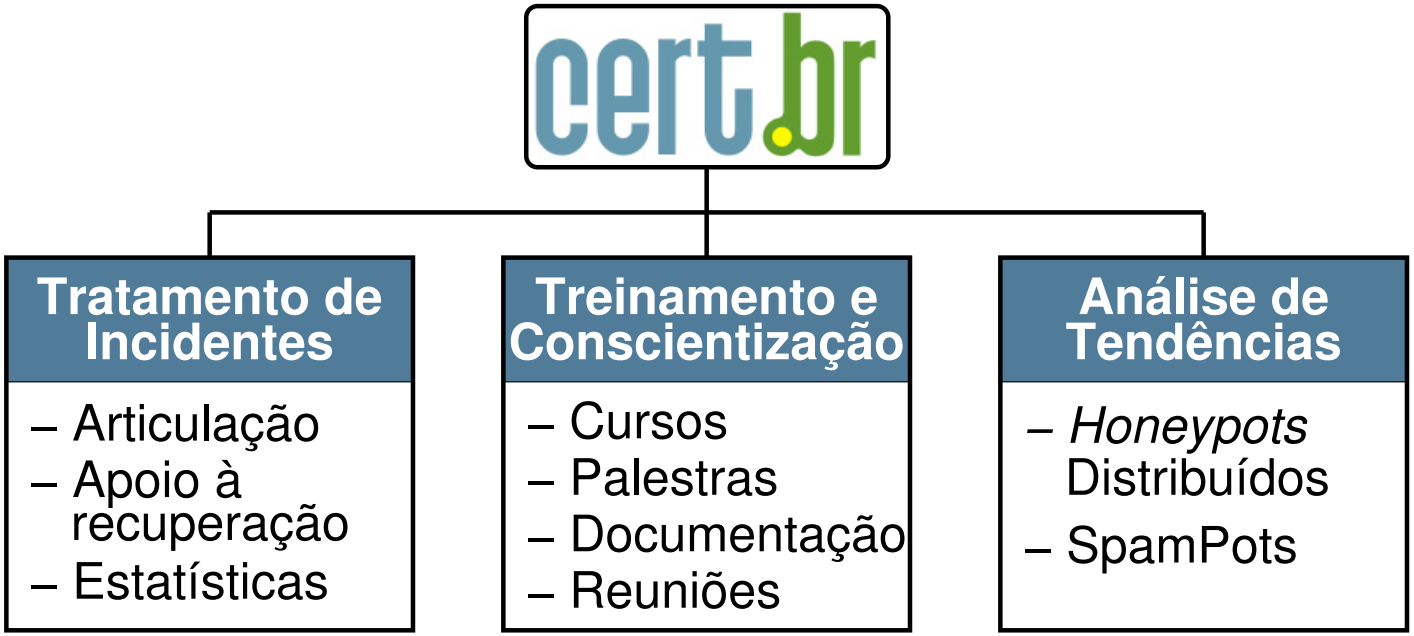
http://www.cgi.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

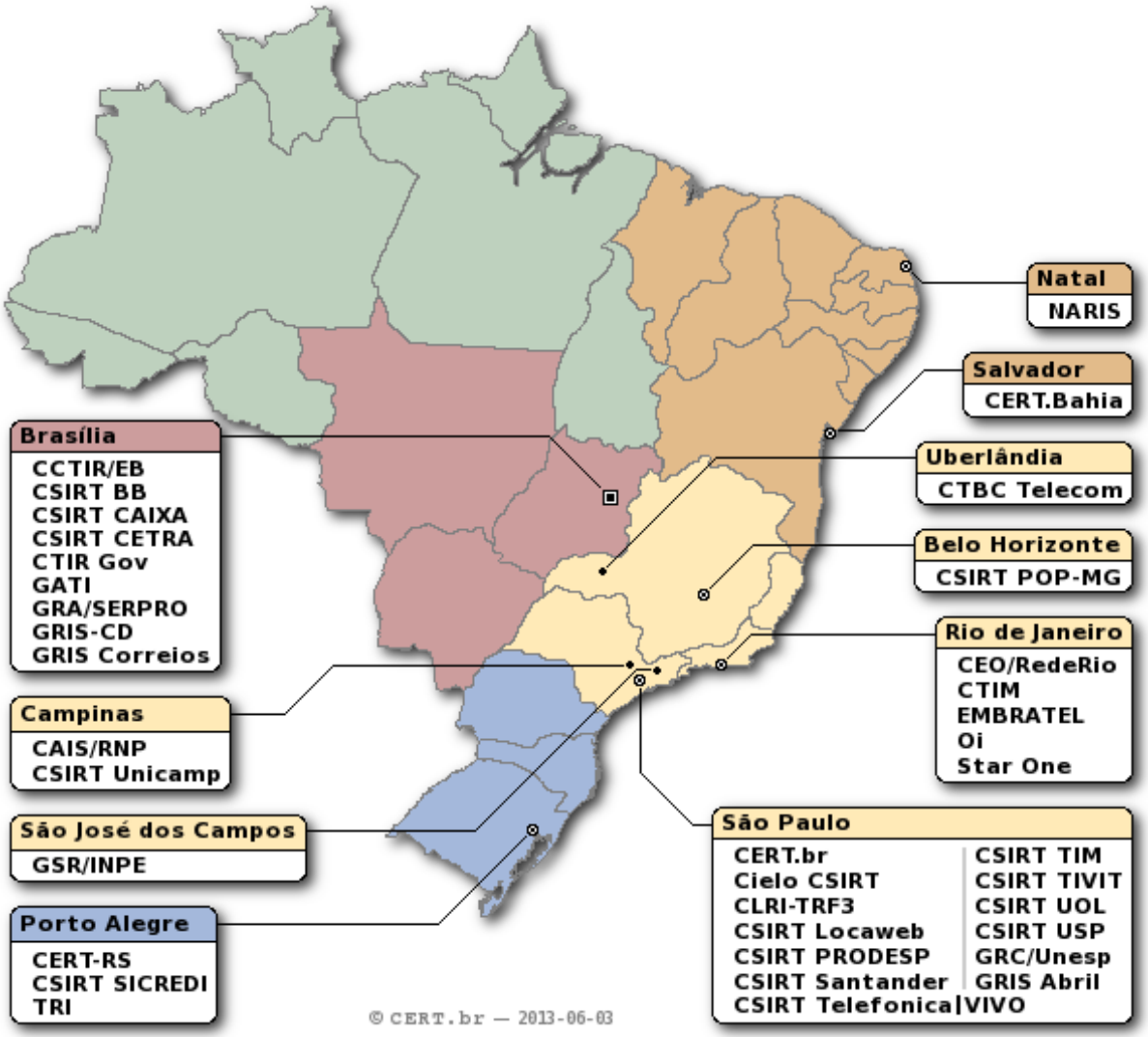
- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

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/

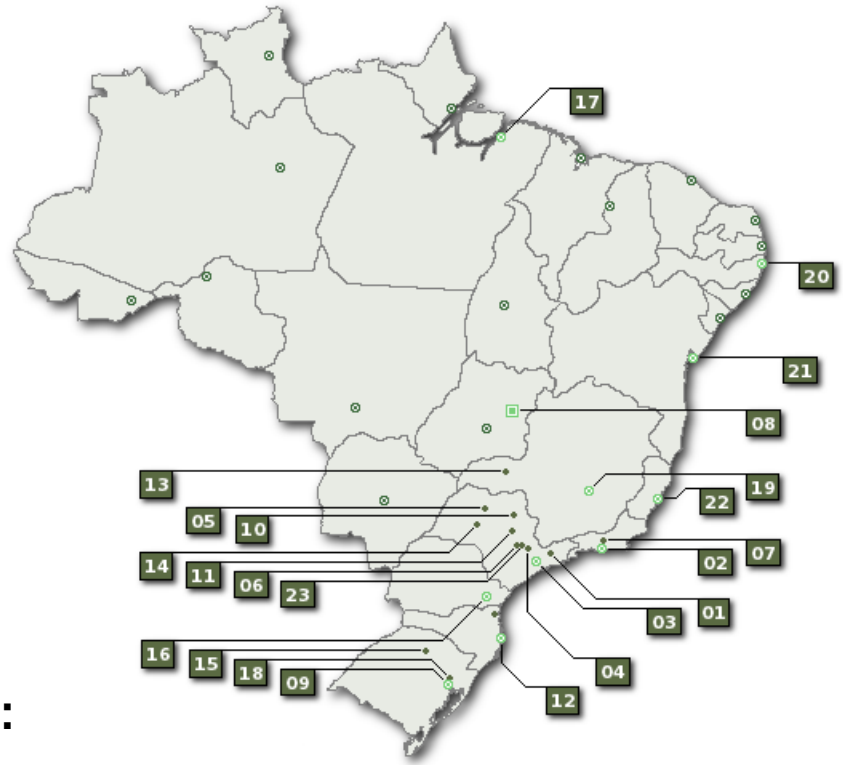
Honeypots Distribuídos

Mapeamento das atividades maliciosas na Internet no Brasil

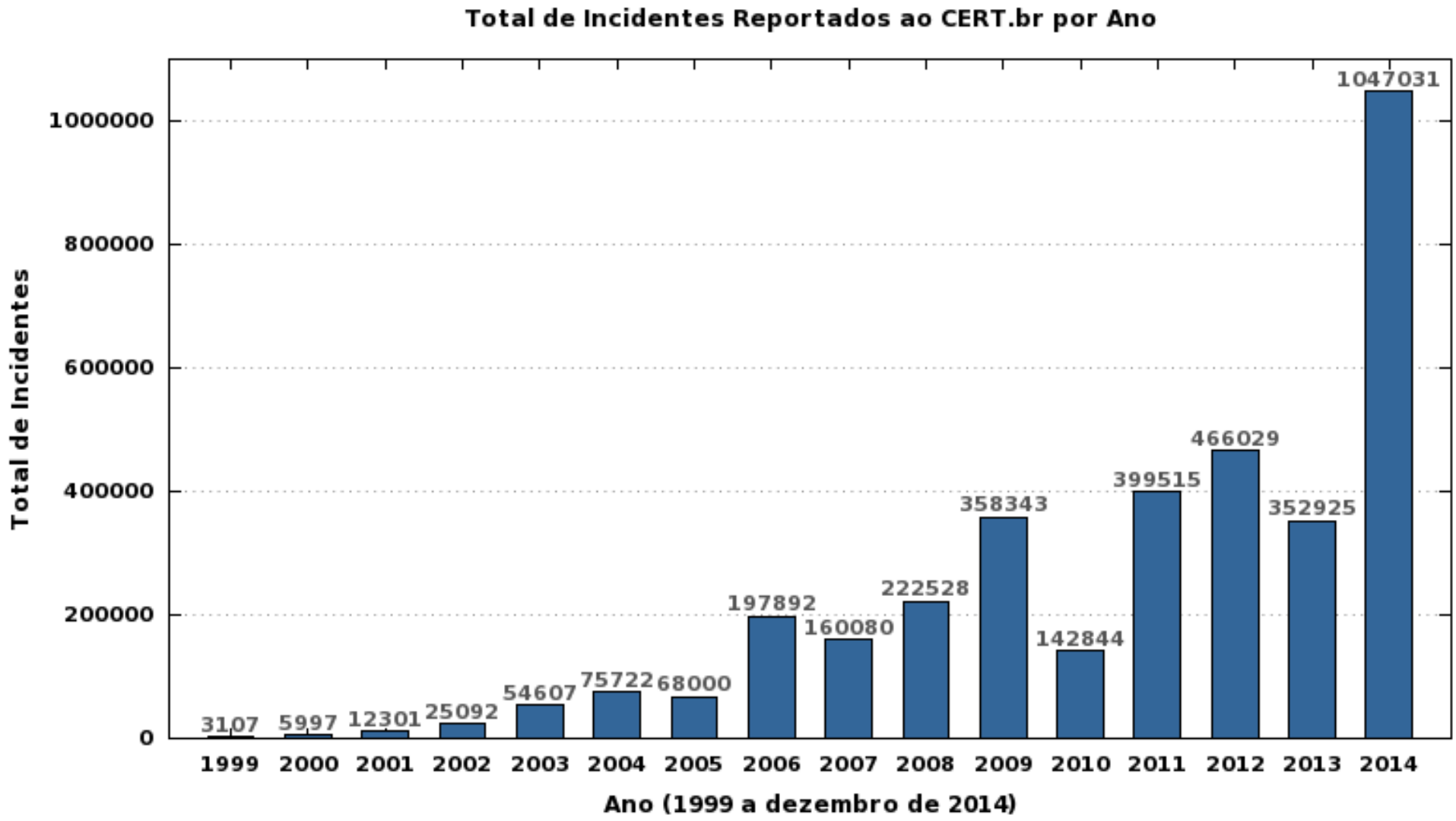
- **55 sensores em 43 redes (universidades, governo, provedores, operadoras e empresas)**

Uso dos dados:

- **Gerar estatísticas públicas sobre tendências**
- **Notificar *sites* brasileiros com problemas**
- **Enviar dados anonimizados**
  - **para CERTs Nacionais, para auxiliar esforços de combate a botnets: Austrália, Polônia, Uruguai, Argentina, Colômbia, Qatar**
  - **Entidades de combate a botnets: Arbor Atlas, Team Cymru, ShadowServer**



Estatísticas CERT.br – 2014



Protegendo suas Contas de Acesso na Internet

cert.br nic.br cgi.br

Agenda

- **Senhas, senhas e mais senhas**
- **Recomendações**
  - O que não utilizar
  - O que utilizar
  - Cuidados ao usar suas senhas
- **Verificação em duas etapas**
- **Outros cuidados**
- **Referências**

Senhas, senhas e mais senhas

cert.br nic.br cgi.br

Senhas

- **Servem para autenticar um usuário**
  - asseguram que você é realmente quem diz ser, e
  - que possui o direito de acessar o recurso em questão

- **Um dos principais mecanismos de autenticação usados na Internet**

Senhas permitem acesso a:

- ***Sites* de:**
  - comércio eletrônico
  - Internet *Banking*
  - notícias
  - redes sociais
  - jogos *online*
- **Serviços de:**
  - *e-mail*
  - hospedagem (de arquivos, nuvem)
- **Dispositivos móveis**
- **Computadores pessoais**
  - compartilhamentos de rede
- **Equipamentos de rede**

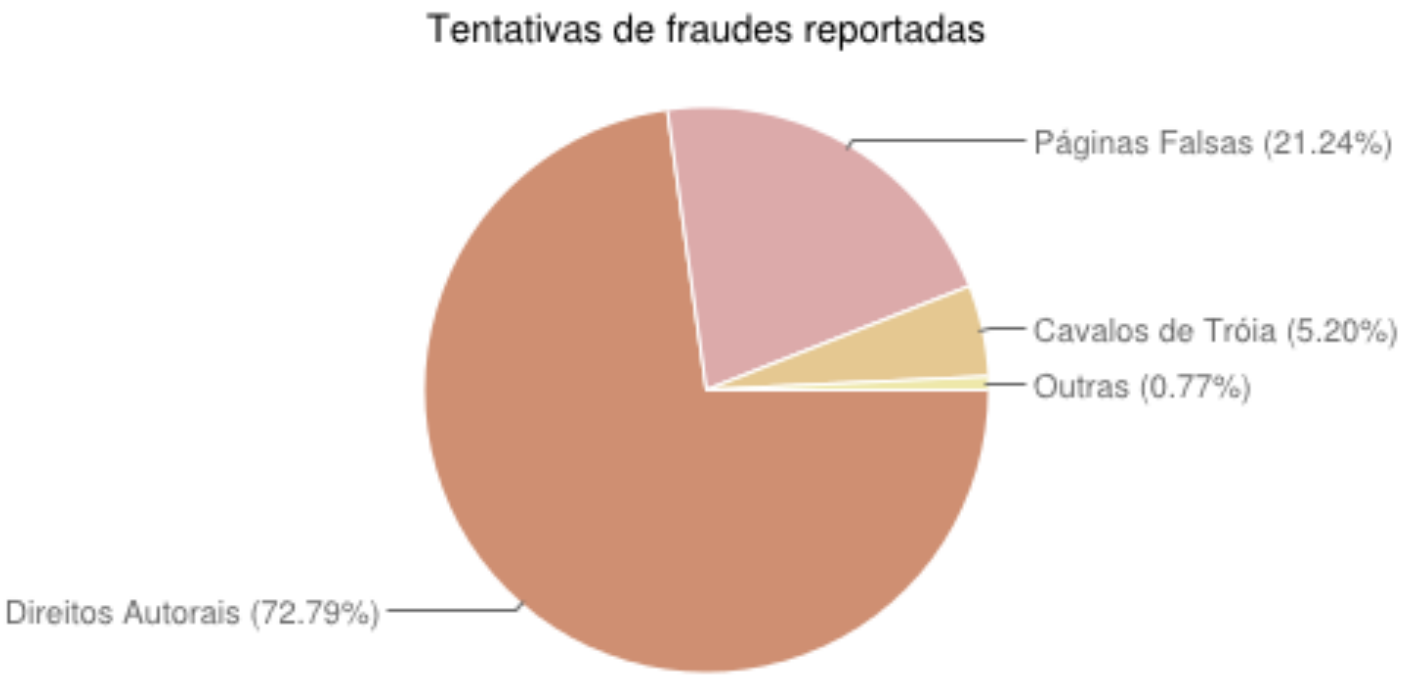
Por que alguém iria querer obter suas senhas?

- **Acessar informações confidencias**
- **Aplicar golpes de engenharia social**
- **Propagar códigos maliciosos**
- **Disseminar *spam***
- **Enviar mensagens contendo *phishing***
- **Impedir o acesso do usuário à conta invadida**
- **Invadir o computador e utilizá-lo para desferir ataques**
- **Invadir o equipamento de rede e mudar as configurações**

Como sua senha pode ser descoberta

- **Por meio:**
  - de tentativas de adivinhação (força bruta)
  - do acesso ao arquivo onde foi armazenada
  - de técnicas de engenharia social
- **Ao ser capturada enquanto trafega na rede, sem estar criptografada (*sniffers*)**
- **Pela observação da movimentação:**
  - dos seus dedos no teclado
  - dos cliques do *mouse* em teclados virtuais
- **Quando usada em:**
  - *sites* falsos (*phishing*)
  - computadores infectados e/ou invadidos

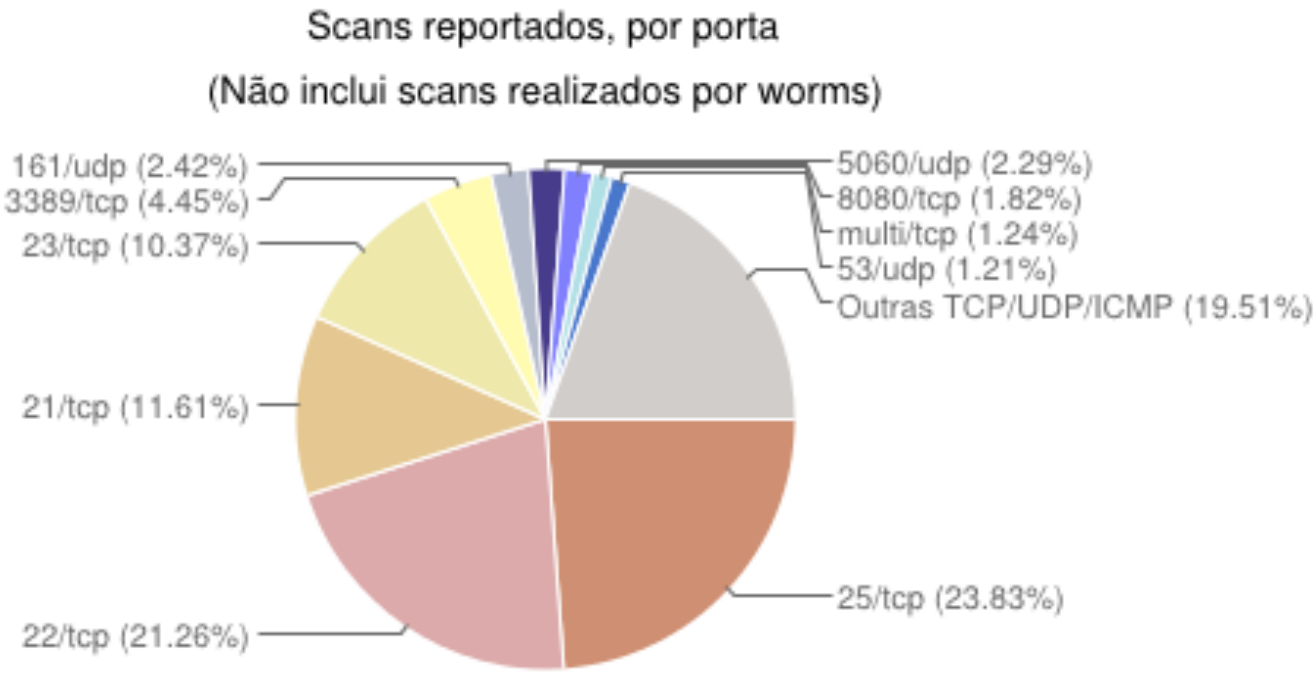
Tentativas de fraude – 2014



Ataques de força bruta

- **Tentativas de adivinhar senhas através de:**
  - palavras existentes em dicionários
    - de diferentes idiomas
    - facilmente obtidos na Internet
  - listas de palavras comumente usadas
  - listas de senhas padrão
  - substituições óbvias de caracteres
  - sequências de teclado
  - informações pessoais
    - coletadas em redes sociais, *blogs*
    - de conhecimento prévio do atacante

Ataques de força bruta – 2014



Recomendações

cert.br nic.br cgi.br

O que não utilizar

cert.br nic.br cgi.br

Evite usar

- **Dados pessoais**
  - nome, sobrenome
  - contas de usuário
  - datas
  - números de documentos, de telefones ou de placas de carros
- **Dados disponíveis em redes sociais e páginas Web**
- **Sequências de teclado**
  - “1qaz2wsx”, “QwerTAsdfG”
- **Palavras presentes em listas publicamente conhecidas**
  - músicas, times de futebol
  - personagens de filmes
  - dicionários de diferentes idiomas

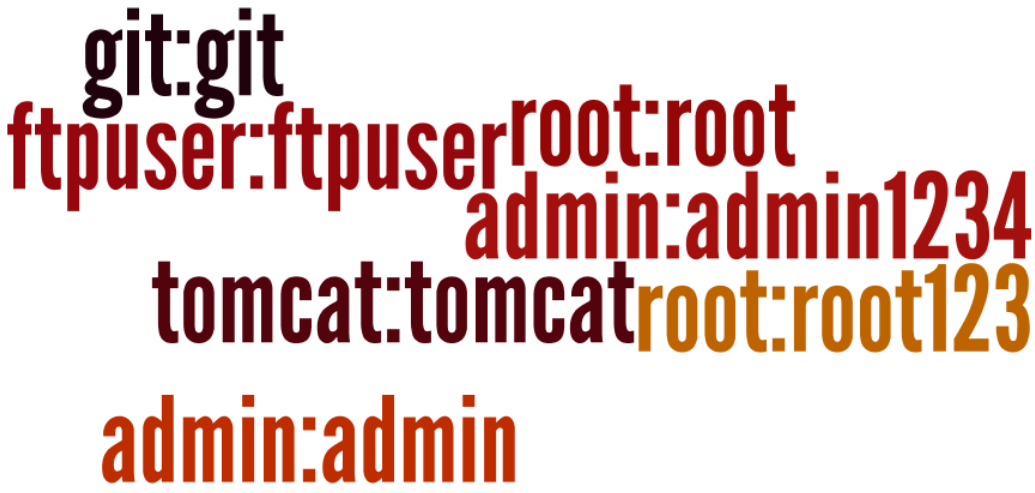
Recomendações / Ataques de força bruta

- **Dados coletados pelo Projeto Honeypots Distribuídos**
- **Referentes a 39/59 sensores - julho a dezembro/2014**
- **Permitem ilustrar o cenário dos ataques de força bruta sobre o serviço de ssh**

Tentativas	100.138.783
Contas únicas	180.390
Senhas únicas	983.045
Contas e senhas	1.331.791

Evite usar dados pessoais

Senha igual a conta	**8.19%**
Senha parte da conta	**4.57%**
% sobre o total	**12.76%**



Evite usar caracteres do mesmo tipo

Apenas dígitos	**13.55%**
Apenas caracteres alfabéticos	**37.94%**
Caracteres alfanuméricos	**28.99%**
Caracteres alfanuméricos e símbolos	**19.46%**
Senha vazia	**0.06%**

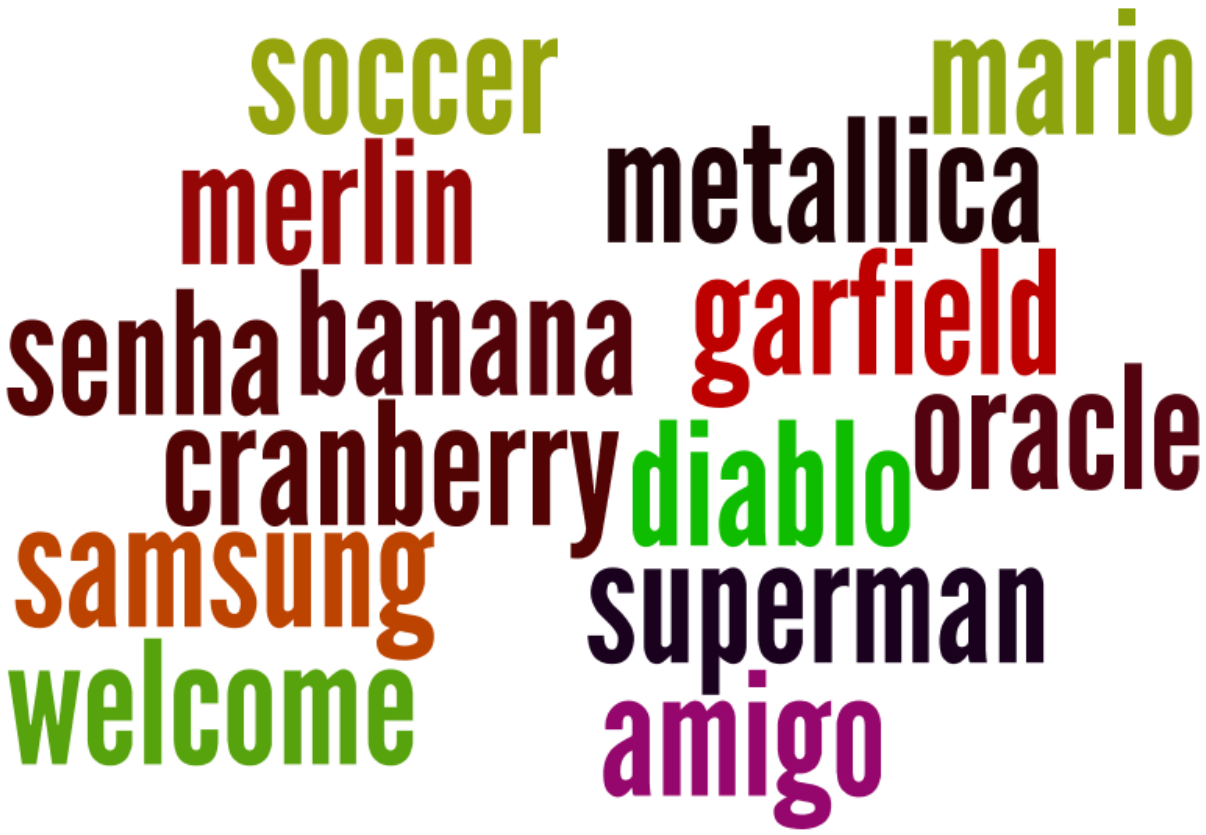
Evite usar sequencias de teclado

Apenas dígitos	**3.71%**
Apenas caracteres alfabéticos	**1.61%**
Caracteres alfanuméricos	**2.03%**
Caracteres alfanuméricos e símbolos	**0.03%**
Porcentagem sobre o total	**7.38%**

Evite usar repetições do mesmo caracter

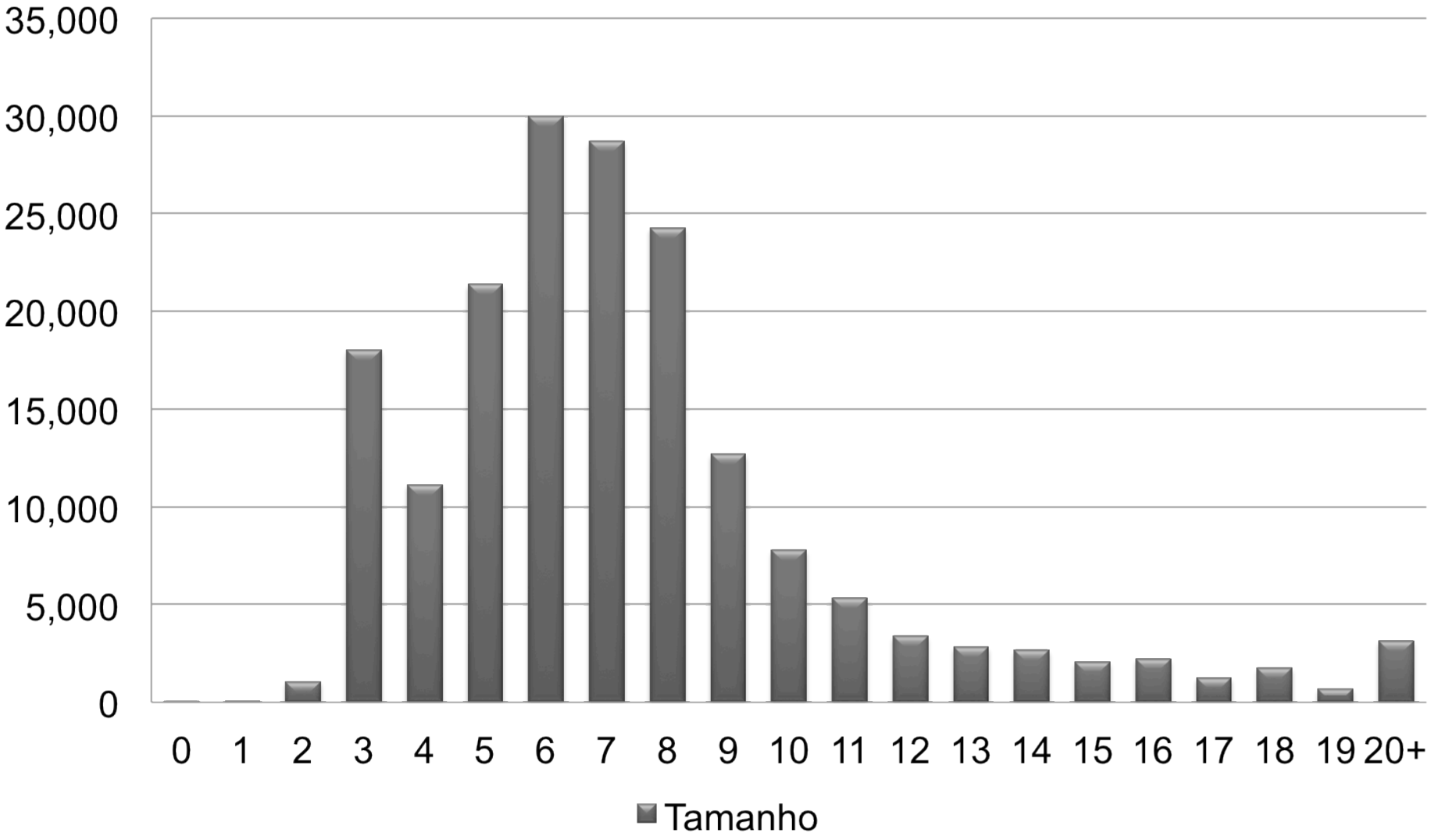
Apenas dígitos	**1.81%**
Apenas caracteres alfabéticos	**0.56%**
Apenas símbolos	**0.11%**
Porcentagem sobre o total	**2.49%**

Evite usar palavras que fazem parte de listas



Evite substituições óbvias de caracteres

Evite usar senhas curtas



Como tentativas podem se tornar invasões

	Projeto Honeypots Distribuídos	Splashdata
1	root	123456
2	123456	password
3	admin	12345
4	password	12345678
5	1234	qwerty
6	12345	123456789
7	root123	1234
8	passw0rd	baseball
9	admin123	dragon
10	abc123	football

11	123	1234567
12	test	monkey
13	oracle	letmein
14	1qaz2wsx	abc123
15	changme	111111
16	12345678	mustang
17	qwerty	access
18	123456789	shadow
19	qwe123	master
20	1q2w3e4r	michael

http://splashdata.com/press/worst-passwords-of-2014.htm

O que utilizar

cert.br nic.br cgi.br

O que utilizar

- **Senhas longas**
  - quanto maior a senha mais difícil será descobrí-la
  - com o uso frequente acabam sendo facilmente digitadas
- **Números aleatórios**
  - quanto mais aleatórios melhor
  - principalmente em sistemas que aceitem exclusivamente caracteres numéricos
- **Diferentes tipos de caracteres**
  - quanto mais “bagunçada” mais difícil será descobri-la

Dicas práticas para elaborar boas senhas

- **Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**

  Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”
  Senha: “?OCbcaRddus”

- **Escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**

  Senha: “1 dia ainda verei os aneis de Saturno!!!”

- **Invente um padrão de substituição próprio**

  Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”
  Frase: “Sol, astro-rei do Sistema Solar”
  Senha: “SS0l, asstrr0-rrei d0 SSisstema SS0larr”

Não use estas senhas

Apenas você pode definir se sua senha é realmente boa

Cuidados ao usar suas senhas

cert.br nic.br cgi.br

Seja cuidadoso ao usar suas senhas

- **Certifique-se de utilizar conexão segura**
- **Não forneça suas senhas para outra pessoa**
  - em hipótese alguma
- **Certifique-se de não estar sendo observado ao digitá-las**
- **Evite utilizar computadores de terceiros**
- **Somente acesse os serviços digitando o endereço diretamente no navegador Web**
  - nunca clicando em *links* existentes em páginas ou mensagens

Recuperação de senhas

- **Questões de segurança**
  - procure criar sua própria questão
  - cuidado com questões pessoais e facilmente adivinháveis

- **Envio por *e-mail***
  - procure alterá-la rapidamente
  - cadastre um *e-mail* que você acesse frequentemente

Métodos de gerenciamento (1/2)

- **Pouco indicados:**
  - usar uma mesma senha para diversos serviços
    - basta que o atacante consiga uma senha para acessar diversas contas
  - salvar no navegador Web
    - podem ser acessadas por códigos maliciosos e atacantes, caso não estejam criptografadas

Métodos de gerenciamento (2/2)

- **Mais indicados:**
  - Anotar em um papel e guardá-lo em local seguro
    - preferível a ter que optar por usar senhas fracas
    - segurança das senhas depende diretamente da dificuldade de acesso ao local onde o papel esta´ guardado
  - Usar serviços de hospedagem de contas/senhas
    - senhas hospedadas em servidores remotos
    - verificar políticas de privacidade
    - garantir que as senhas trafeguem criptografada
  - Usar programas gerenciadores de contas/senhas
    - senhas gravadas em arquivo local
    - acessadas através de uma chave mestra
    - não esqueça sua chave mestra
    - segurança das demais senhas depende da chave mestra

Quando alterar a senha

- **Imediatamente:**
  - ao desconfiar que ela tenha sido descoberta
  - ao usá-la em um computador comprometido
  - caso o dispositivo onde ela está armazenada seja furtado
- **Rapidamente:**
  - quando usar um padrão de formação e desconfiar que uma delas tenha sido descoberta (trocar também o padrão)
  - ao adquirir equipamentos acessíveis via rede
- **Regularmente:**
  - nos demais casos
  - periodicidade de troca depende:
    - de quanto a senha é exposta
    - de quão boa ela é

Verificação em duas etapas

cert.br nic.br cgi.br

Verificação em duas etapas (1/3)

- **Também chamada de:**
  - *two-factor authentication*
  - aprovação de *login*
  - verificação ou autenticação em dois fatores
  - verificação ou autenticação em dois passos

- **Recurso opcional oferecido por diversos serviços:**
  - *Webmail*
  - redes sociais
  - Internet *Banking*
  - armazenamento em nuvem (*cloud*)

Verificação em duas etapas (2/3)

- **Ao ser habilitada**
  - permite aumentar a segurança de sua conta
  - pode ser desabilitada caso não seja mais desejada
- **Torna mais difícil o acesso indevido de contas de usuário**
- **Para que o acesso ocorra é necessário que o atacante realize com sucesso duas etapas**
  - primeira etapa: senha do usuário
  - segunda etapa: informações adicionais

Verificação em duas etapas (3/3)

- **Segunda etapa pode envolver:**
  - algo que apenas você sabe
    - outra senha
    - perguntas de segurança
    - número PIN
    - alguma informação pessoal
  - algo que apenas você possui
    - código de verificação
    - cartão de senhas bancárias
    - *token* gerador de senhas
    - acesso a um determinado computador ou dispositivo móvel
  - algo que você é
    - informações biométricas
      - impressão digital, palma da mão, rosto, olho

Principais tipos

- **Código de verificação**
- **Código de verificação específico**
- ***Token* gerador de senhas**
- **Cartão de segurança**
- **Dispositivo confiável**
- **Lista de código reserva/*backup***
- **Chave de recuperação**

Tipos – Código de verificação

- **Código individual criado pelo serviço**
- **Enviado de forma que apenas você possa recebê-lo**
  - *e-mail,* chamada de voz, mensagem SMS para o telefone cadastrado
- **Pode ser gerado por um aplicativo autenticador**

- **<u>Cuidados a serem tomados:</u>**
  - mantenha seus dados para recebimento sempre atualizados
    - números de telefones celulares alternativos podem ser cadastrados
    - assegure-se de estar de posse do telefone celular, caso tenha configurado:
      - o envio via SMS
      - o uso do aplicativo autenticador
  - aplicativo autenticador deve ser usado em casos onde não é possível receber mensagens SMS
  - tarifas de recebimento de SMS podem ser aplicadas por sua operadora

Tipos – Código de verificação específico

- **Código gerado para aplicativos que não suportam a verificação em duas etapas**

- **<u>Cuidados a serem tomados:</u>**
  - caso perca o acesso ao seu dispositivo móvel:
    - revogue os códigos específicos gerados para os acessos realizados por meio dele

Tipos – *Token* gerador de senhas

- **Chave eletrônica**
- **Tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade**
- **Cada código é válido por um determinado período**
  - geralmente alguns segundos
  - após esse tempo um novo código é gerado
  - código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo

- **<u>Cuidados a serem tomados:</u>**
  - guarde seu *token* em um local seguro
  - nunca informe o código mostrado no *token* por *e-mail* ou telefone
  - caso perca seu *token* ou ele seja furtado:
    - avise imediatamente o responsável pelo serviço no qual ele é usado

Tipos – Cartão de segurança

- **Cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta**

- **<u>Cuidados a serem tomados:</u>**
  - guarde seu cartão em um local seguro
  - nunca forneça os códigos do cartão por *e-mail* ou telefone
  - forneça apenas uma posição do seu cartão a cada acesso
  - verifique se o número de identificação do cartão apresentado pelo serviço corresponde ao que está no seu cartão
    - caso sejam diferentes entre em contato com o serviço
  - desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição do cartão

Tipos – Dispositivo confiável

- **Computador ou dispositivo móvel usado para acessar suas contas**
- **No primeiro acesso:**
  - pode ser necessário inserir um código de segurança
  - ele não será necessário nos demais, pois seu dispositivo será "lembrado", caso você assim o configure

- **<u>Cuidados a serem tomados:</u>**
  - não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles
  - pode ser necessário habilitar a opção de *cookies* em seu navegador Web para que seu dispositivo seja memorizado

Tipos – Lista de códigos reserva/*backup*

- **Lista de códigos que devem ser usados de forma sequencial e uma única vez**

- **<u>Cuidados a serem tomados:</u>**
  - anote ou imprima a lista e a mantenha em um local seguro
  - não a armazene em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes
    - caso não esteja criptografada
  - caso perca a lista ou desconfie que alguém a acessou você deve gerá-la novamente ou revogá-la
    - anulando assim a anterior

Tipos – Chave de recuperação

- **Número gerado pelo serviço quando você ativa a verificação em duas etapas**
- **Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis**

- **<u>Cuidados a serem tomados:</u>**
  - anote ou imprima a chave e a mantenha em um local seguro
  - não a deixe anotada em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes
    - caso não esteja criptografada
  - caso perca ou desconfie que alguém acessou a sua chave você deve gerá-la novamente
    - substituindo assim a anterior

Outros cuidados

cert.br nic.br cgi.br

Dados pessoais

- **Mantenha seu cadastro atualizado**
  - dados pessoais podem ser solicitados aleatoriamente para checar a sua identidade
  - seu endereço de correspondência pode ser usado para o envio de tokens e cartões de segurança
  - dados pessoais e perguntas de segurança podem ser solicitados
    - caso você desabilite a verificação em duas etapas

Mantenha seus equipamentos seguros (1/2)

- **Mantenha sempre a versão mais recente de todos os programas instalados**
- **Aplique todas as atualizações**
  - principalmente as de segurança
- **Utilize e mantenha atualizados mecanismos de segurança:**
  - *antispam*
  - antivírus
  - *firewall* pessoal
- **Configure-os para solicitar senha na tela inicial**
  - cadastre uma senha de acesso que seja bem elaborada
  - configure-os para aceitarem senhas complexas (alfanuméricas)

Mantenha seus equipamentos seguros (2/2)

- **Fique atento a mensagens:**
  - recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links
  - que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;

- **Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens**

- **Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente. Ela pode:**
  - ter sido forjada
  - ter sido enviada de contas invadidas, de perfis falsos

Proteja seus dispositivos móveis

- **Mantenha controle físico sobre eles**
  - principalmente em locais de risco
  - procure não deixá-los sobre a mesa
  - cuidado com bolsos e bolsas
- **Seja cuidadoso ao instalar aplicativos de terceiros**
- **Em caso de perda ou furto:**
  - remova-os da lista de dispositivos confiáveis
  - revogue autorizações concedidas para aplicativos instalados
  - cadastre um novo número de celular
  - se tiver configurado a localização remota:
    - apague remotamente os dados armazenados

Proteja seus equipamentos de rede

- **Atualize o *firmware***
  - seja cuidadoso ao fazer a atualização
  - verifique no site do fabricante os detalhes do procedimento
  - se necessário peça ajuda a alguém mais experiente
- **Altere a senha de administração**
  - use senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais, palavras conhecidas e sequências de teclado
  - lembre-se de guardar tanto a senha nova como a original
  - restaure a senha original somente quando necessário

A segurança da Internet depende de todos.

Faça a sua parte!

Referências

cert.br nic.br cgi.br

Educação de Usuários:
Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no site, via *Twitter* e RSS
http://cartilha.cert.br/

Cartilha de Segurança para Internet
Fascículos

Organizados de forma a facilitar a difusão de conteúdos específicos:

- **Redes Sociais**
- **Senhas**
- **Comércio Eletrônico**
- **Privacidade**
- **Dispositivos Móveis**
- ***Internet Banking***
- **Computadores**
- **Códigos Maliciosos**
- **Verificação em Duas Etapas**
- **Redes**

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

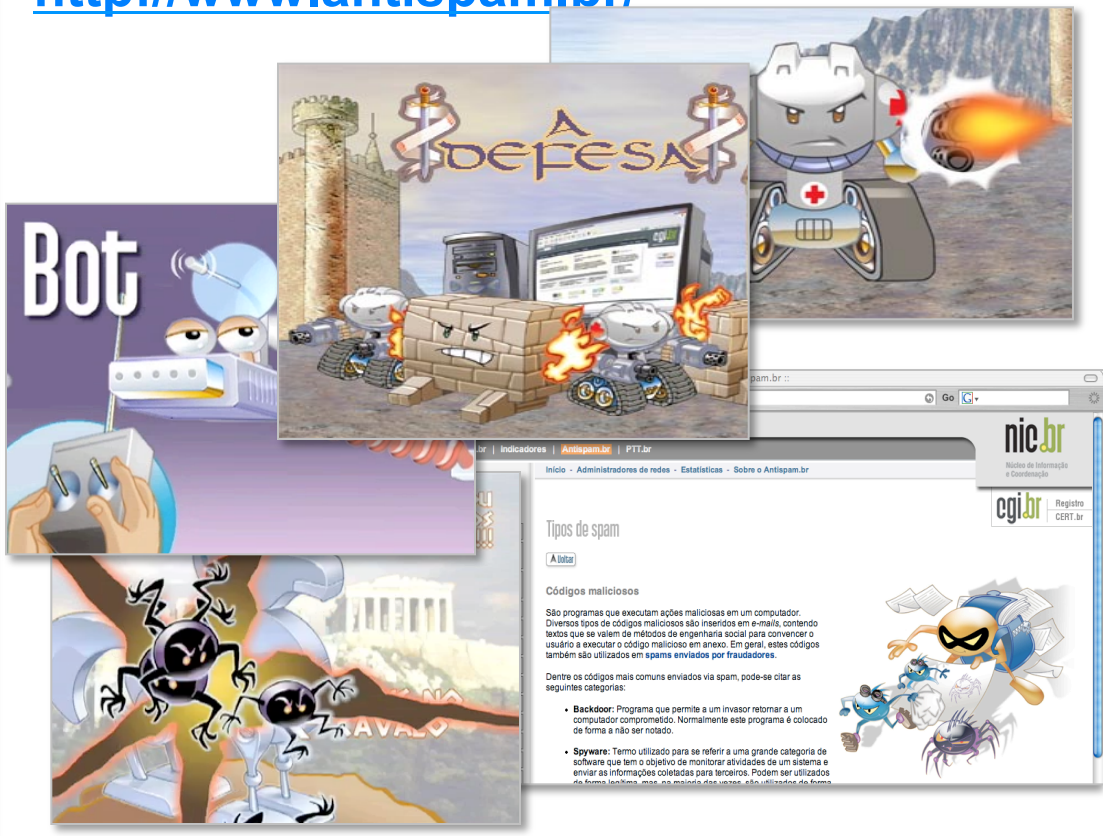
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/



Obrigada

www.cert.br

miriam@cert.br

@certbr

17 de junho de 2015

nic.br cgi.br

www.nic.br | www.cgi.br