nic.br cgi.br | cert.br

Belo Horizonte, MG

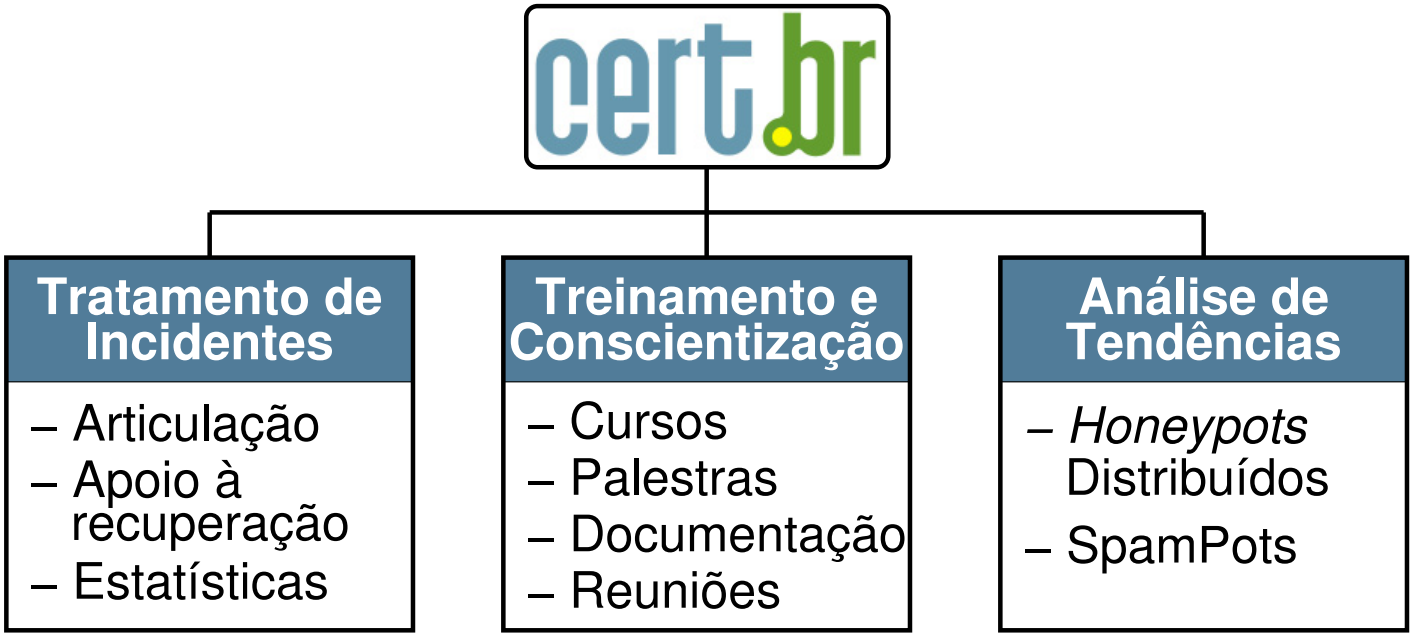
26 de outubro de 2015

Em dia com a Segurança da Informação

Segurança em Dispositivos Móveis

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

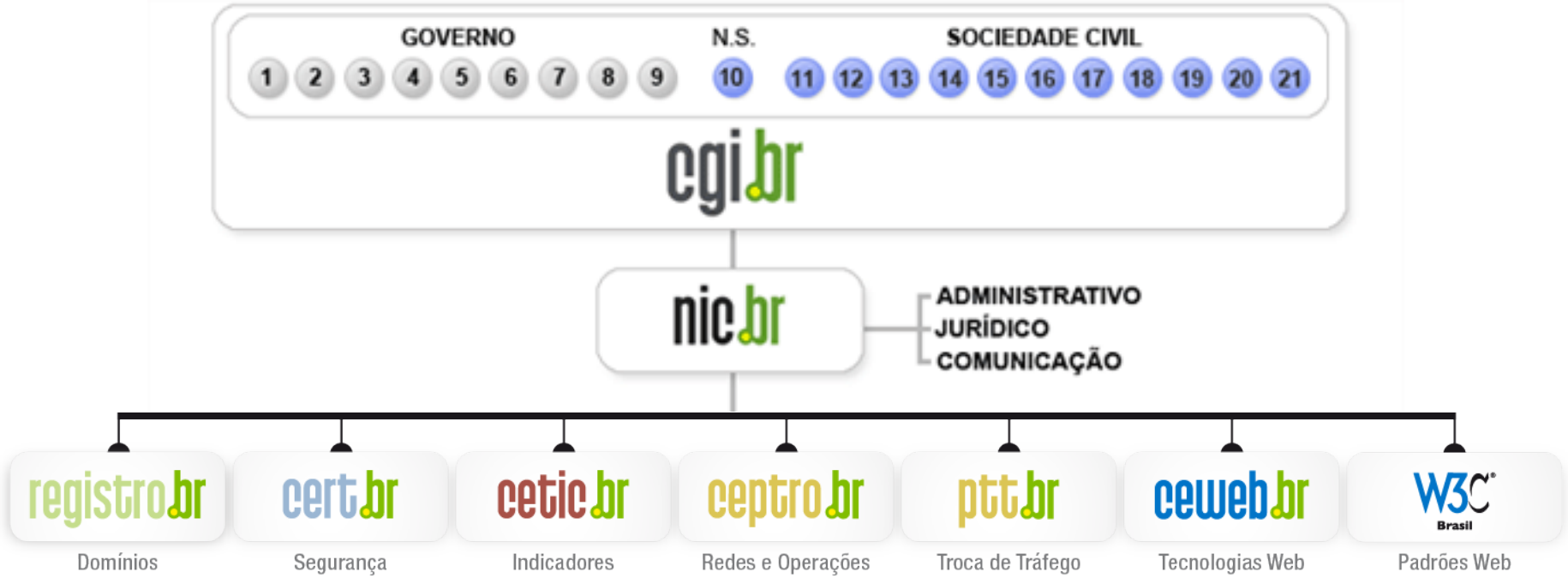
The Honeynet PROJECT

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/

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

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

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/

Segurança em Dispositivos Móveis

Agenda

- **Dispositivos móveis**
- **Riscos principais**
- **Cuidados a serem tomados**
- **Referências**

Dispositivos móveis

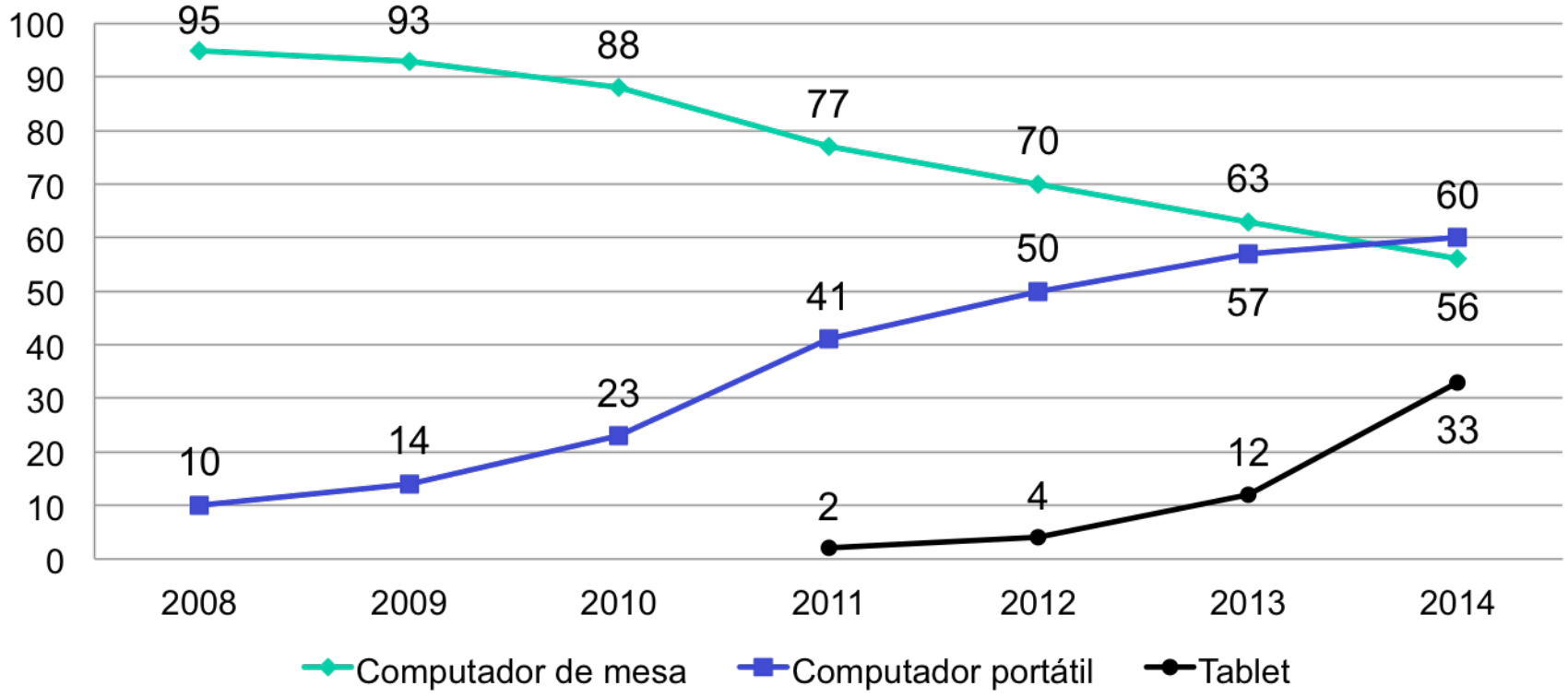
- ***Tablets*, *smartphones*, celulares, *notebooks*, etc.**
- **Principais características:**
  - mobilidade
  - peso e portabilidade
  - cada vez mais populares
  - auxílio em tarefas cotidianas e profissionais
  - uso individualizado
  - grande quantidade informações
  - conectividade (Wi-Fi, *bluetooth*, infravermelho, 3G, 4G)

Dispositivos móveis
Funcionalidades

- **Similares às dos computadores pessoais**
  - navegação Web, *Internet Banking*, *e-m*ails e redes sociais
- **Extras**
  - GPS
  - câmera
  - controle remoto
  - pagamento móvel
  - *mobile banking*
  - autenticação – verificação em duas etapas
  - *cloud computing*
  - BYOD – *Bring Your Own Device*
  - NFC – *Near Field Communication*
  - integração com *gadgets*
    - IoT, saúde, automação residencial

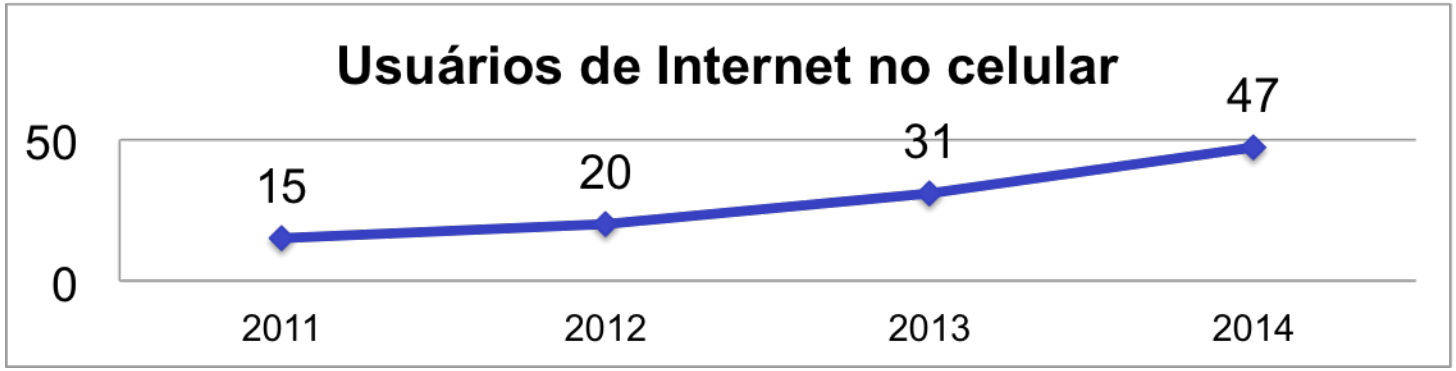
TIC Domicílios 2014 - Residências

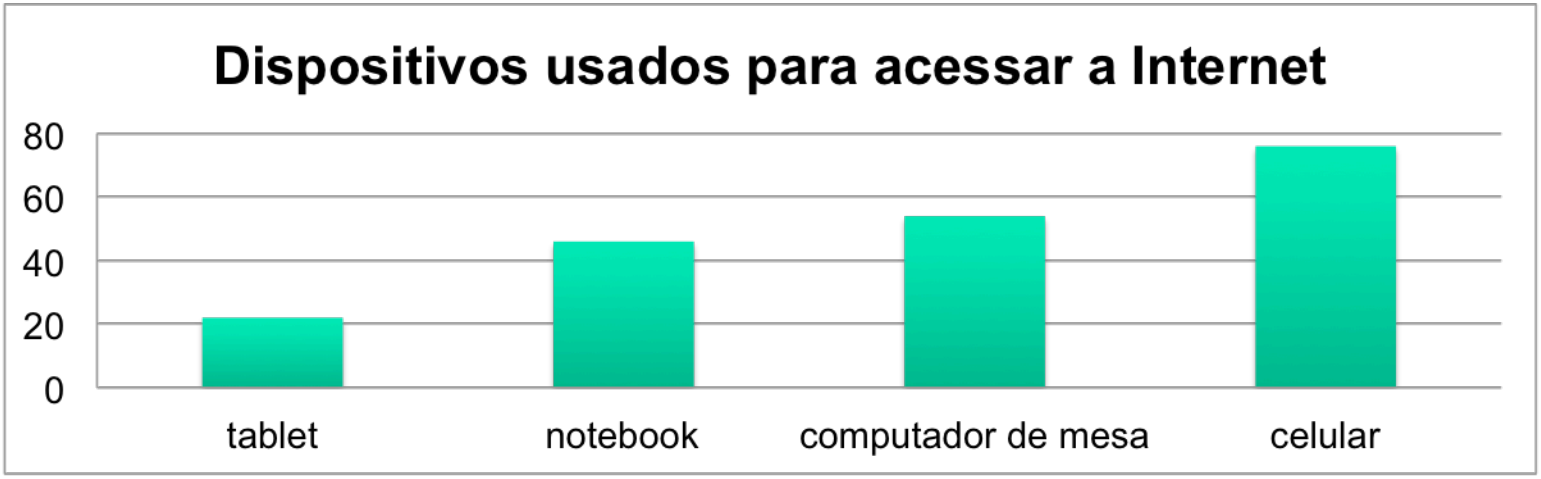
- **Tendência à mobilidade**
  - Wi-Fi presente em 66% das moradias com acesso à Internet
- **Tendência à portabilidade e ao uso individualizado**



TIC Domicílios 2014 - Uso do celular

- **81,5 mi de usuários de Internet no celular**
- **84% acessam todos ou quase todos os dias**





Riscos principais

Dispositivos móveis X Computadores pessoais

- **Riscos similares**
  - códigos maliciosos
  - *phishing*
  - acesso a conteúdos impróprios ou ofensivos
  - contato com pessoas mal-intencionadas
  - perda de dados
  - dificuldade de manter sigilo
  - furto de identidade

- **DM mais atraentes para pessoas mal-intencionadas**
  - pelas características e novas possibilidades de uso que oferecem

- **Usuários costumam achar que não correm riscos**

Maior possibilidade de perda e furto

- tamanho reduzido
- alto valor financeiro
- representam status
- constantemente em uso
- usados em locais públicos
- atraem atenção de assaltantes
- perda da noção de espaço/tempo
- facilmente esquecidos e perdidos

Dependência e uso excessivo

- **“Nomofobia”**
  - *no-mobile phobia* – medo de ficar sem dispositivo móvel
- **FOMO**
  - *Fear Of Missing Out* – medo de estar perdendo algo
- **Depressão:**
  - por usar excessivamente as redes sociais
  - por falta de uso das redes sociais
- **Problemas de socialização**
- **Síndrome do toque fantasma**
- **Jogos *online***
- **Diversas outras mudanças comportamentais**

Códigos maliciosos/*Malware*

- **Vírus, *worm*, *trojan*, *bot*, *ransomware*, etc.**
- **Recebidos por meio de:**
  - mensagens SMS/MMS
  - *e-mails*
  - WhatsApp, redes sociais, etc.
- **Dispositivo infectado pode:**
  - ter os dados coletados
  - ter os dados apagados
  - disseminar *spam*
  - participar de ataques na Internet
  - fazer parte de *botnets*

Aplicativos maliciosos

- **Muitos aplicativos sendo desenvolvidos**
  - diferentes autores e funcionalidades
  - dificuldade de manter controle
- **Podem existir aplicativos:**
  - intencionalmente desenvolvidos para:
    - executar atividades maliciosas
    - coletar dados dos aparelhos
  - não intencionalmente
    - erros de implementação
    - desenvolvidos sem requisitos de segurança
    - utilizem ambientes de desenvolvimento comprometidos
- **Podem estar disponíveis nas “lojas” de cada sistema**

Exploração de vulnerabilidades

- **Diversas vulnerabilidades sendo descobertas nos sistemas operacionais e aplicativos**
- **Fragmentação de versões**
  - customizações feitas por fabricantes e operadoras
- **Dificuldade em manter sistemas atualizados**

Invasão de privacidade

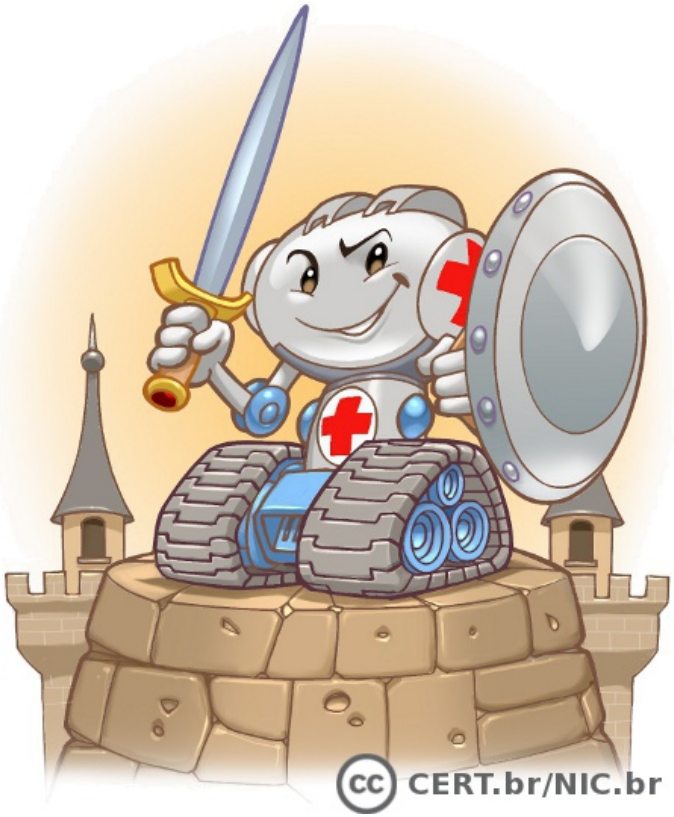
- **Intencional:**
  - dispositivos estão sempre à mão
  - uso generalizado
- **Localização fornecida por aplicativos de GPS**
- **Dados pessoais coletados por:**
  - aplicativos
  - códigos maliciosos
  - atacantes

Vazamento de informações

- **Grande quantidade de informações pessoais gravadas:**
  - na nuvem, sem preocupações com segurança
  - localmente:
    - sem criptografia
    - sem *backup*
    - problemas com assistência técnica e furto/roubo

- **Rápida substituição de modelos sem a devida exclusão das informações gravadas**

Cuidados a serem tomados



Antes de adquirir um dispositivo

- **Verifique a política de atualizações oferecida pelo fabricante do aparelho e/ou operadora**
- **Observe os mecanismos de segurança oferecidos**
  - diferentes modelos e fabricantes
  - escolha o que considerar mais seguro
- **Caso opte por um modelo já usado**
  - restaure as configurações de fábrica/originais antes de usá-lo
- **Não adquira um dispositivo:**
  - ilegalmente desbloqueado (*jailbreak*)
  - com permissões de acesso alteradas
    - ação ilegal
    - violação dos termos de garantia
    - comprometimento da segurança e de funcionamento

Ao usar o dispositivo (1/5)

- **Instale e mantenha atualizados mecanismos de segurança**
  - antivírus (deve ser instalado antes de qualquer outro aplicativo)
  - *antispam*
  - *antimalware*
  - *firewall* pessoal

- **Mantenha seu dispositivo seguro:**
  - com a versão mais recente de todos os programas instalados
  - com todas as atualizações aplicadas

- **Não siga links recebidos via mensagens eletrônicas**
  - SMS, *e-mails*, redes sociais, etc.

Ao usar o dispositivo (2/5)

- **Mantenha-o sempre com a tela bloqueada**
  - deslizar
    - protege apenas de uso acidental
  - desenho
    - cuidado com o rastro
  - reconhecimento facial
  - PIN
  - senha
  - impressão digital

- **Configure:**
  - senha de acesso ao cartão SIM
  - para que o PIN seja solicitado quando o telefone for ligado

Ao usar o dispositivo (3/5)

- **Mantenha controle físico**
  - principalmente em locais de risco
  - procure não deixá-lo sobre a mesa
  - cuidado com bolsos/bolsas em ambientes públicos

- **Proteja sua privacidade**
  - seja cuidadoso ao:
    - publicar sua geolocalização
    - permitir que aplicativos acessem seus dados pessoais

- **Respeite a privacidade alheia**

Ao usar o dispositivo (4/5)

- **Proteja suas senhas**
  - cadastre senhas de acesso bem elaboradas
  - se possível, configure-o para aceitar senhas complexas (alfanuméricas)
  - use senhas longas, com diferentes tipos de caracteres
  - não utilize:
    - sequências de teclado
    - dados pessoais, como nome, sobrenome e datas
    - dados que possam ser facilmente obtidos sobre você
  - evite salvar senhas nos aplicativos
  - evite reutilizar senhas

Ao usar o dispositivo (5/5)

- **Proteja seus dados**
  - faça backups periódicos
  - mantenha informações sensíveis em formato criptografado
  - use conexão segura quando transmitir dados confidenciais
    - senhas
    - número de cartão de crédito

- **Ao usar sistemas de armazenamento em nuvem**
  - seja cuidadoso ao elaborar as senhas
  - verifique as informações de último acesso
  - **use verificação em duas etapas**

Ao instalar aplicativos

- **Procure obter aplicativos de fontes confiáveis**
  - lojas confiáveis
  - *site* do fabricante
- **Escolha aplicativos:**
  - bem avaliados
  - com grande quantidade de usuários
- **Verifique com antivírus antes de instalar o aplicativo**
- **Observe as permissões para execução**
  - elas devem ser coerentes com a finalidade do aplicativo
    - um aplicativo de jogos, por exemplo, não necessariamente precisa ter acesso à sua lista de chamadas

Ao acessar redes Wi-Fi

- **Não permita a conexão automática a:**
  - redes públicas
  - redes já visitadas
    - atacante pode configurar rede com o mesmo nome e sem saber você estará acessando essa rede falsa
- **Lembre-se de apagar as redes que você visitou**
  - isso ajuda a preservar a sua privacidade
- **Procure usar redes que ofereçam criptografia WPA2**
  - evite usar WEP e WPA
- **Algumas redes públicas redirecionam a navegação no primeiro acesso para um site de autenticação**
  - essa autenticação serve apenas para restringir os usuários e não garante que as informações trafegadas serão criptografadas

Ao usar o *bluetooth*

- **Mantenha as interfaces inativas e habilite quando usar**
- **Configure as interfaces para que a visibilidade seja "Oculto" ou "Invisível"**
- **Altere o nome padrão do dispositivo**
  - evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo
- **Altere a senha (PIN) padrão do dispositivo**
  - seja cuidadoso ao elaborar a nova
- **Fique atento ao receber mensagens solicitando autorização ou PIN**
  - não responda se não tiver certeza que está se comunicando com o dispositivo correto

Ao se desfazer do dispositivo

- **Apague todas as informações nele contidas**
- **Restaure as configurações de fábrica**

Previna-se para casos de perda ou furto

- **Configure-o previamente para que:**
  - seja localizado/rastreado e bloqueado remotamente
  - uma mensagem seja mostrada na tela
  - o volume seja aumentado ou que saia do modo silencioso
  - os dados sejam apagados após certo número de tentativas de desbloqueio sem sucesso (CUIDADO COM CRIANÇAS)
- **Anote o IMEI:**
  - *International Mobile Equipment Identity*
  - identificação global e única para cada aparelho
    - ligar para *#06#
    - etiqueta atrás da bateria
    - caixa do celular

Em caso de perda ou furto

- **Informe:**
  - a sua operadora
    - solicite o bloqueio do seu número (chip)
  - a empresa onde você trabalha
    - caso haja dados e senhas profissionais nele armazenadas
- **Bloqueie:**
  - IMEI
  - cartão de crédito cujo número esteja gravado
- **Altere as senhas nele armazenadas**
- **Ative:**
  - a reprodução do som
  - a localização remota, caso a tenha configurado
    - apague remotamente os dados nele gravados
    - **não tente recuperá-lo sozinho**

BYOD – Cuidados

- **Para as empresas:**
  - crie uma política de segurança sobre os direitos e deveres da empresa e dos funcionários relativos:
    - a posse do dispositivo
    - aos aplicativos instalados
    - aos dados armazenados
    - aos custos de acesso à Internet ou a ligações feitas
    - as responsabilidades de reposição em caso de perda ou furto
    - a exclusão de dados em caso de demissão
  - criar rede separada para os dispositivos
- **Para os funcionários:**
  - verifique a política da empresa sobre o uso de dispositivos próprios para acessar dados profissionais
  - seja bastante cuidadoso ao usar esses dispositivos

Referências

cert.br nic.br cgi.br

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/

Fascículos da Cartilha de Segurança para Internet

Visa facilitar a difusão de conteúdos específicos por multiplicadores:

- 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

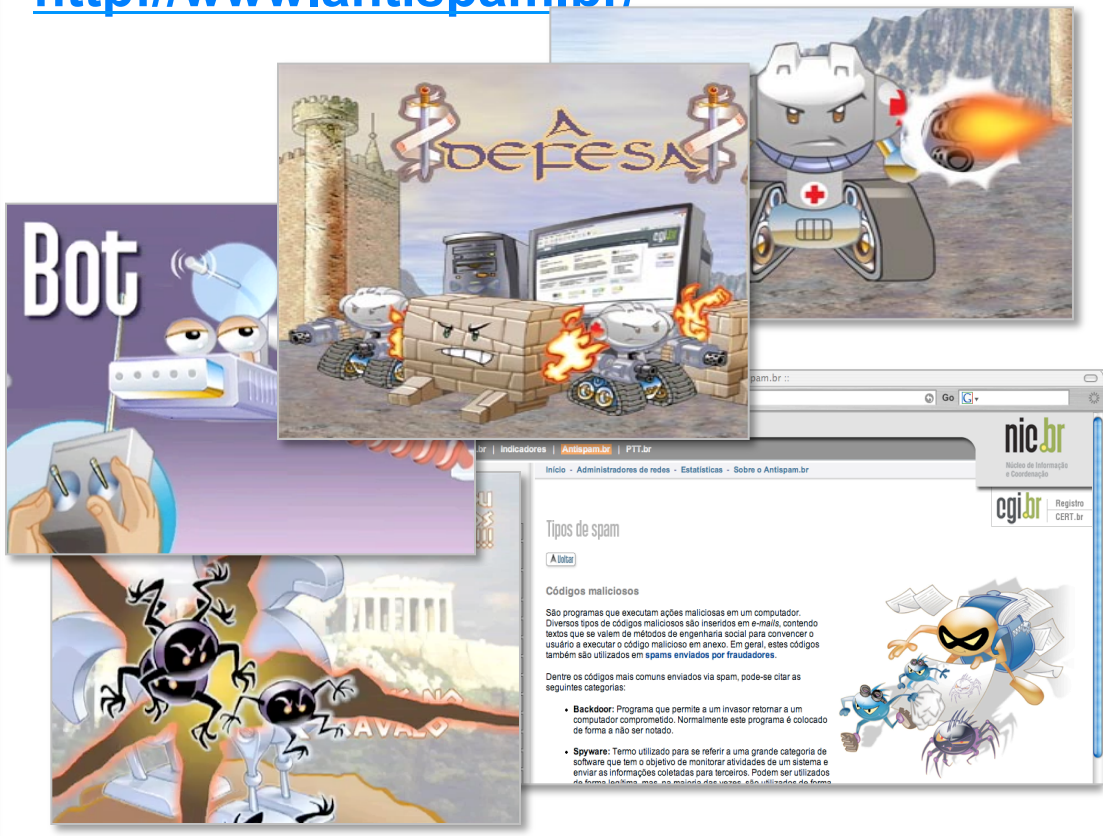
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

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

26 de outubro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br