



Segurança em Redes Sociais

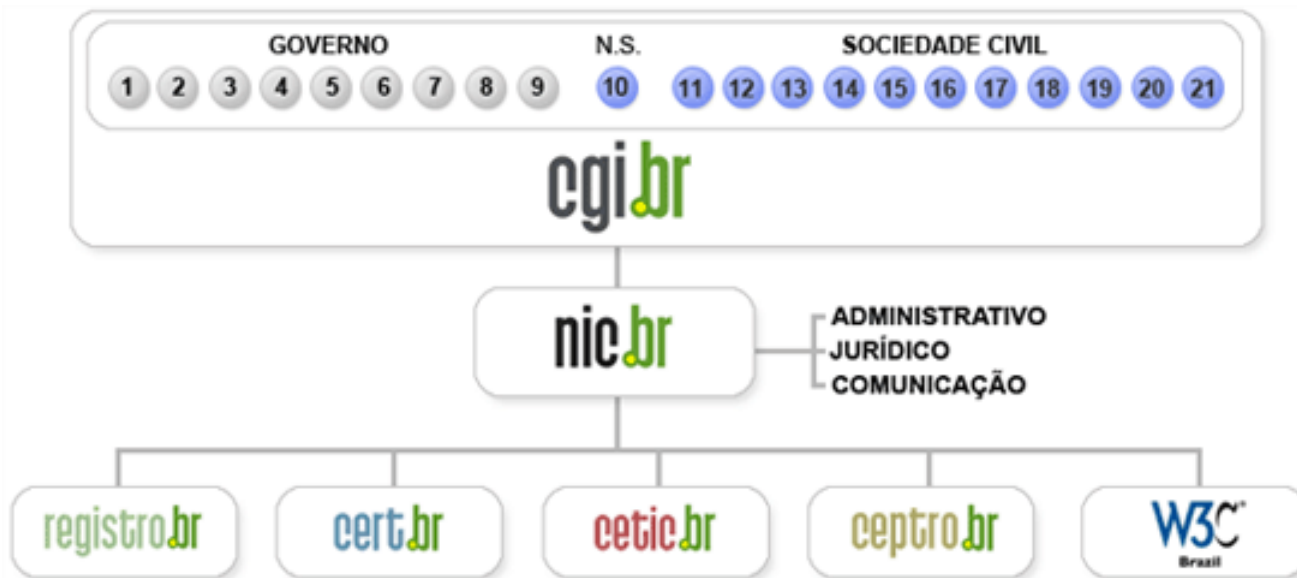
Lucimara Desiderá
lucimara@cert.br



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

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

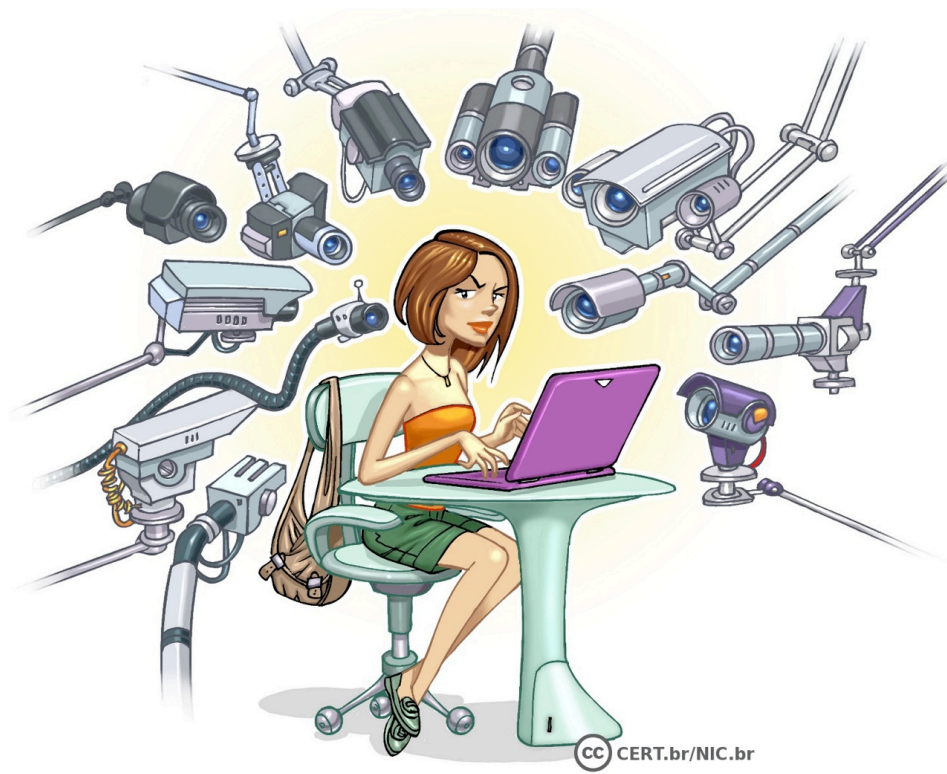
Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- 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;

Agenda

- **Redes sociais**
 - **Características principais**
 - **Riscos principais**
 - **Cuidados a serem tomados**

Redes Sociais



Redes sociais

- **Redes de relacionamento que permitem que os usuários:**
 - forneçam informações sobre si
 - acessem informações sobre outros usuários
 - criem listas de contatos
 - utilizem mecanismos de comunicação
 - se agrupem, de acordo com afinidades, características, interesses e objetivos em comum
- **Conteúdo totalmente gerado pelos próprios usuários**
 - **Diário público**

Redes sociais no Brasil

- **comScore (dezembro/2011):**
 - Facebook: 36,1 milhões (assume liderança)
 - Orkut: 34,4 milhões
 - Windows Live: 13,3 milhões
 - Twitter: 12,5 milhões
 - Google+: 4,3 milhões
 - LinkedIn: 3,1 milhões
- **Socialbakers (setembro/2012 - Brasil):**
 - 57 milhões de usuários – #2 no mundo
- **Especial Mobile, IBOPE Nielsen Online (abril/2012):**
 - 77% visitam redes sociais

Características principais



Características principais

- **Rápida velocidade de propagação de informações**
- **Grande quantidade de usuários**
- **Facilidade de acesso**
- **Grande quantidade de informações pessoais**
- **Dificuldade de exclusão de informações**
- **Dificuldade de controle sobre as informações**
- **Tempo que as informações ficam disponíveis**

Riscos principais



CC CERT.br/NIC.br

Riscos principais – Na mídia (1/2)

- **“A cada 40 minutos acontece um crime relacionado ao Facebook” (TechTudo 10/06/2012)**
 - **“A grande maioria dos casos envolve assédio sexual ou intimidação via Internet (*bullying*)”**
 - **“Entre os crimes mais cometidos estão assassinato, estupro, crimes sexuais contra crianças, assalto, sequestro e ameaças de morte”**
- **“Facebook revela que 83 milhões de seus usuários são *fakes*” (TechTudo – 02/08/2012)**

Riscos principais – Na mídia (2/2)

- “Filho de Eugene Kaspersky é sequestrado após publicar dados em rede social” (Olhar Digital – 19/05/2011)
- TIC Crianças 2010 – CETIC.br
 - “O uso da Internet desacompanhado é alto entre as crianças (39%)”
 - “21% dos pais declara não realizar nenhum tipo de restrição ou controle do filhos no uso da Internet.”

- Harold Wigginbottom (maio/2009)

Wiggy107 Amped for South America trip to fire up Colombian sales force! Landing Tues 5/12 around 4:10pm
 10:13 AM May 10 from web

Wiggy107 Airport time = reading time. Briefcase locked & loaded w/ Q4 projections and R&D reports. Then Tetris!
 7:01 AM May 12 from TwitterBerry

Wiggy107 Did I leave front door unlocked? Will find out when I'm back next week LOL! Preboarding 1st class now!
 7:42 AM May 12 from TwitterBerry

Wiggy107 Wheels down! Bogota airport kinda sketchy. Hooray, admin musta remembered car service -- driver has sign for Wiggy107!
 4:19 PM May 12 from TwitterBerry

Wiggy107 NO SE PREOCUPEN, TODO ESTA BIEN. POR FAVOR ENVIEN MUCHO \$\$\$ A ESTA OFICINA DE LA WESTERN UNION...
 5:31 PM May 15 from TwitterBerry

Riscos principais (1/4)

Invasão de privacidade

- **Síndrome da celebridade: quantidade X qualidade**
- **Pequenos pedaços de informação podem nada significar até serem agregados**
 - hábitos, rotina, estilo de vida e condição social
 - procura de emprego
- **Privacidade deixou de ser uma questão individual**
 - não adianta um usuário restringir se os amigos divulgam
- **Mudanças nas políticas de privacidade e nos recursos dos *sites*.**

Riscos principais (2/4)

Furto de identidade e uso indevido de informações

- **Quanto mais informações um usuário disponibiliza mais fácil é para um impostor furtrar a sua identidade**
- **Criação de perfil falso**
 - **golpes de engenharia social**
 - **coletar informações de sua rede**
 - **aproximar-se de outras pessoas**
- **Criação de contas falsas**
- **Invasão de contas**

Riscos principais (3/4)

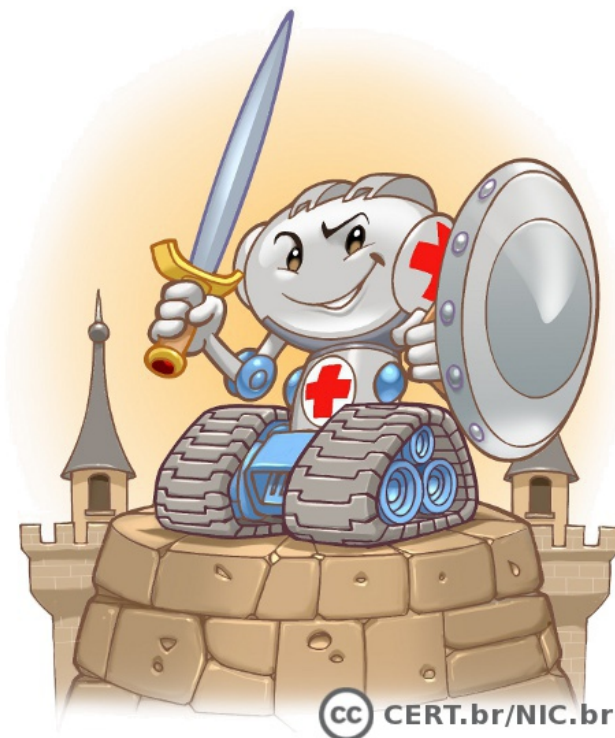
Danos à imagem e à reputação

- **Calúnia e difamação**
 - podem colocar em risco a vida profissional
 - podem trazer danos psicológicos e de convívio social
- **Frases fora de contexto podem ser tornar dúbias e/ou ofensivas**
- **Dificuldade em diferenciar assuntos pessoais de profissionais**
- **Funcionários e consumidores insatisfeitos**

Riscos principais (4/4)

- **Vazamento de informações**
 - danos a imagem
 - perda de vantagem competitiva
 - perdas financeiras
- **Recebimento de mensagens disseminando códigos maliciosos, *phishing*, *spam***
- **Acesso a conteúdos impróprios ou ofensivos**
- **Contato com pessoas mal-intencionadas**
- **Disponibilização de informações para criminosos, que podem ser usadas:**
 - em tentativas de sequestro
 - para furto de bens

Cuidados a serem tomados



Preserve a sua privacidade

- **Considere que você está em um local público**
- **Pense bem antes de divulgar (não há como voltar atrás)**
- **Use as opções de privacidade oferecidas pelos *sites***
 - procure ser o mais restritivo possível
- **Mantenha seu perfil e seus dados privados**
- **Restrinja o acesso ao seu endereço de *e-mail***
- **Seja seletivo ao aceitar seus contatos**
- **Seja cauteloso ao dar acesso à aplicativos**
 - permissões independem das opções configuradas no perfil
- **Seja cuidadoso ao se associar a grupos e comunidades**
- **Não acredite em tudo que você lê**

Cuidados ao fornecer sua localização

- **Seja cuidadoso ao divulgar fotos e vídeos**
 - ao observar onde foram gerados pode ser possível deduzir sua localização
- **Não divulgue:**
 - planos de viagens
 - por quanto tempo ficará ausente de sua residência
- **Ao usar redes sociais baseadas em geolocalização:**
 - faça *check-in* apenas em locais movimentados
 - faça *check-in* ao sair do local, ao invés de quando chegar

Respeite a privacidade alheia

- **Evite falar sobre as ações, hábitos e rotina de outras pessoas**
- **Não divulgue sem autorização:**
 - **imagens em que outras pessoas apareçam**
 - **mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso**
- **Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público**

Proteja o seu perfil (1/3)

- **Seja cuidadoso ao elaborar as suas senhas**
 - **fácil de lembrar x difícil de ser deduzida**
 - **use senhas longas, compostas de diferentes tipos de caracteres**
 - **não utilize sequências de teclado, contas, palavras de dicionários, dados pessoais (disponíveis na redes sociais)**
 - **elabore senhas distintas para acessar diferentes serviços**
 - **avale o risco envolvido**
 - **não misture pessoal x profissional**
 - **crie seu próprio padrão/algoritmo**

Proteja o seu perfil (2/3)

- **Seja cuidadoso ao usar as suas senhas**
 - não exponha nem compartilhe
 - não armazene no navegador sem usar criptografia
 - evite utilizar em computadores de terceiros
 - adote um mecanismo de gerenciamento de senhas
 - papel guardado em local seguro
 - programa específico
 - arquivo criptografado (não esqueça a chave mestra)
 - troque suas senhas regularmente
 - troque imediatamente caso suspeite que tenha sido comprometida.

Proteja o seu perfil (3/3)

- **Habilite as notificações de *login***
- **Seja cauteloso ao instalar e dar acesso à aplicativos**
 - código malicioso
 - acesso adicional aos configurados no perfil
- **Lembre-se sempre de fechar a sua sessão (*logout*)**
- **Denuncie aos responsáveis pela rede social caso identifique abusos, tais como:**
 - imagens indevidas
 - perfis falsos
 - *spam*

Proteja o seu computador (1/2)

- **Mantenha seu computador seguro com:**
 - todos os programas instalados nas versões mais recentes
 - todas as atualizações aplicadas
- **Utilize e mantenha atualizados mecanismos de segurança**
 - *antispam*
 - *antimalware*
 - *firewall* pessoal

Proteja o seu computador (2/2)

- **Desconfie de mensagens recebidas**
 - mesmo que tenham sido enviadas por conhecidos
 - podem ter sido enviadas de contas falsas ou invadidas
- **Seja cuidadoso ao acessar *links* reduzidos**
 - use complementos que permitam que você expanda o *link*, antes de clicar sobre ele

Proteja a sua vida profissional

- **Cuide da sua imagem profissional**
- **Antes de divulgar uma informação**
 - **avalie se ela pode atrapalhar o seu emprego atual**
 - **avalie se ele pode atrapalhar um processo seletivo futuro**
 - **lembre-se que ela poderá ser acessada por seus chefes e colegas de trabalho**
 - **observe se ela não fere o código de conduta da sua empresa**

Proteja a sua empresa

- **Crie um código de conduta**
- **Informe os funcionários sobre:**
 - os riscos de uso das redes sociais
 - as regras de acesso
 - o comportamento esperado, referente a:
 - divulgação de informações corporativas (sigilosas ou não)
 - emissão de opiniões que possam comprometer a empresa
- **Invista em treinamento**
- **Cuide da imagem**
 - observe a opinião de clientes e consumidores
 - acompanhe ações que envolvam o nome da empresa

Mais informações (1/2)

Cartilha de Segurança para Internet

<http://cartilha.cert.br/>



RSS

<http://cartilha.cert.br/rss/cartilha-rss.xml>



Twitter

<http://twitter.com/certbr>

Mais informações (2/2)

Portal Internet Segura

<http://www.internetsegura.br/>



Campanha Antispam.br

<http://www.antispam.br/>



Perguntas?

Lucimara Desiderá

lucimara@cert.br

- CGI.br - Comitê Gestor da Internet no Brasil
<http://www.cgi.br/>
- NIC.br - Núcleo de Informação e Coordenação do .br
<http://www.nic.br/>
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
<http://www.cert.br/>

cert.br
15 ANOS