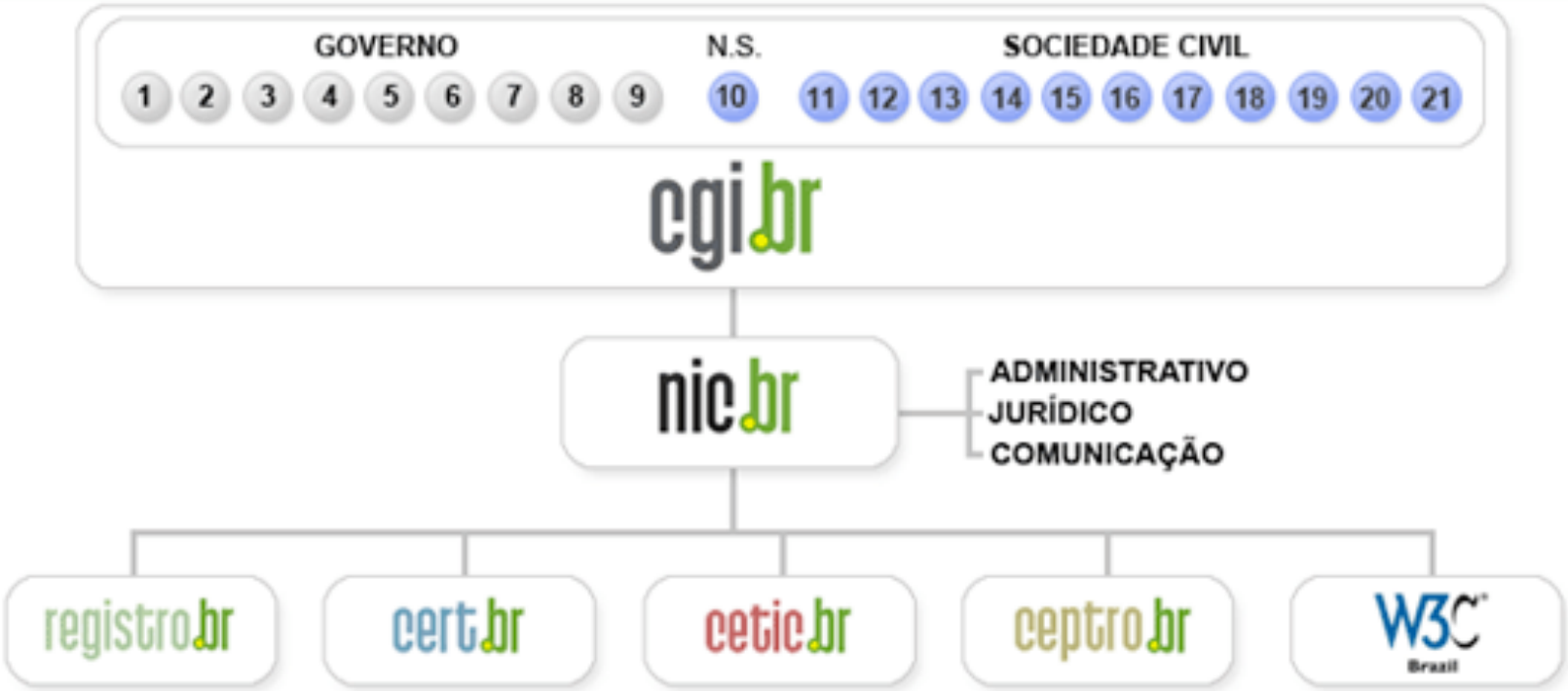
Princípios de Segurança da Informação

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

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

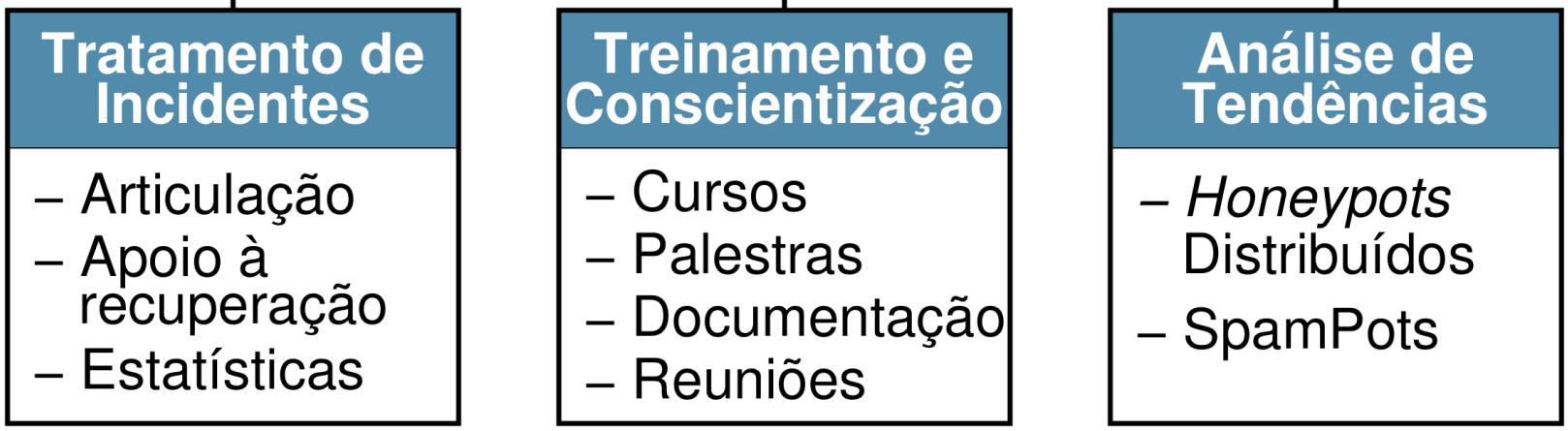
Comitê Gestor da Internet no Brasil – CGI.br

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;**

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

CERT.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 de segurança**
- **Prover a coordenação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones**
- **Auxiliar novos CSIRTs a estabelecerem suas atividades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**

Agenda

- O cenário atual de ataques e ameaças na Internet
- Como e Onde Proteger
- Desafios

Cenário Atual

"It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class."

Inspector John Bonfield
Chicago Herald, 1888

Fonte: "*The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*"

ISBN-13: 978-0802716040

Evolução dos Ataques na Última Década

Mudança no enfoque dos atacantes:

- **Ataques a usuários finais**
  - **fraudes, *bots*, *spyware*, etc**
- **Motivação financeira cresce conforme cresce o uso da Internet pela sociedade**

Características das tentativas de fraude com objetivos financeiros:

- **Majoritariamente envolvem *spams***
  - **em nome das mais variadas instituições e com tópicos diversos**
  - **com *links* (URLs) para códigos maliciosos (cavalos de tróia)**
- **Páginas falsas estão voltando a ter números significativos**
- ***Drive-by downloads* sendo usados intensamente no Brasil**
  - **alguns dos casos publicados na mídia:**

    ***sites* principais da Vivo, da Oi e da Ambev**

Fatores que Contribuem para este Cenário

Há grande motivação para ter usuários como alvo e não as empresas:

- Tem pouco conhecimento sobre a tecnologia
  - a tecnologia é muito complexa
- É muito difícil entender o que é necessário para se proteger

Fatores de comportamento também contribuem:

- O uso do termo "virtual" leva muitos a encarar o que ocorre na Internet como fora da vida "real"
- Informações antes restritas ao círculo familiar e/ou de amigos, agora estão *online*
  - twitter, orkut, facebook, etc…

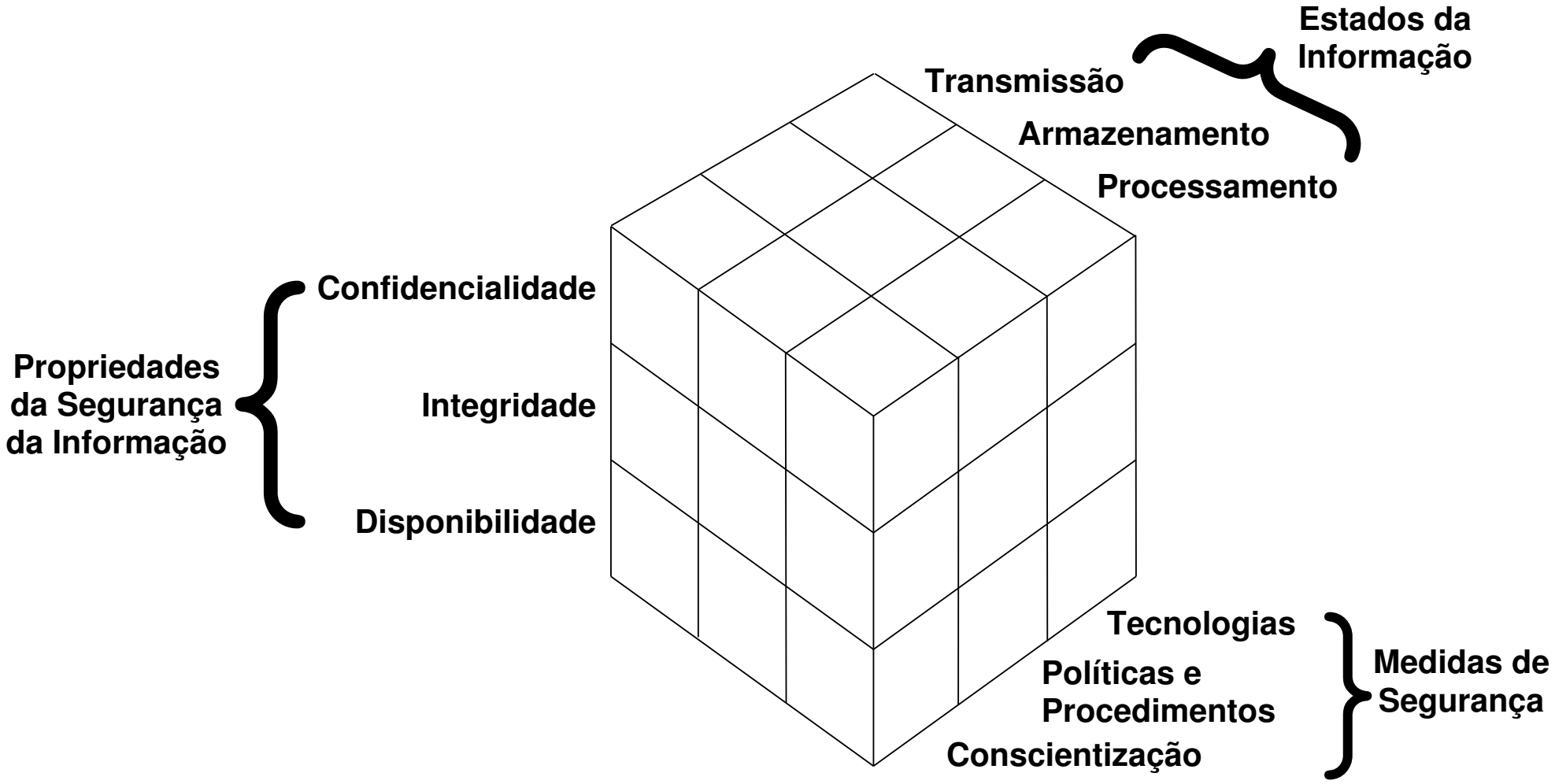
Como e Onde Proteger

"Worries about security of telegraphic money transfers were holding back the development of on-line commerce – 'The opportunity for fraud has been the chief obstacle,' declared the Journal of the Telegraph in 1872."

Fonte: "*The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*"

ISBN-13: 978-0802716040

As Informações Estão em Diversos Locais e a Segurança Depende de Múltiplos Fatores



Especialmente para garantir confidencialidade (e privacidade) é necessario ter controle de acesso, ter logs de quem teve acesso, checar permissões, etc.

Desafios

O que favorece o sucesso dos ataques?

Uma base muito grande de computadores com *software* desatualizado/vulnerável sendo ativamente abusada por atacantes

- **Especialmente em países em desenvolvimento**
- **Usuários**
  - **tem dados furtados**
  - **pagam a conta do uso da Internet por criminosos**

As pessoas não compreendem o risco de

- **Colocar seus dados *online***
- **Compartilhar seu dia-a-dia em público**
- **Não entendem que não é possível ter privacidade e ao mesmo tempo compartilhar as informações em fóruns públicos**

"*Security vs. Privacy*"?

- **Grande parte das contramedidas são tomadas sem considerar as questões de privacidade**
  - **A maioria sequer funciona ou melhora a segurança, apenas aumenta o controle**
    - **Ex.: "*Unique IDs*", "*RFID passports*", banalização da biometria**
- **Como resultado, medidas válidas e necessárias são questionadas em nome da privacidade**
  - **Mesmo que não afetem a privacidade**
- **Não é necessário comprometer a privacidade para ter mais segurança**
  - **mas registros de eventos (*logs*) são necessários tanto para garantir confidencialidade quanto disponibilidade**
- **Muitas das quebras de privacidade não tem nada a ver com segurança da informação**

O desconhecimento do problema e das soluções gera um embate que não deveria existir.

O Que Fazer?

- **Riscos sempre vão existir, em qualquer meio**
- **Educação é chave**
  - **desenvolvedores**
  - **administradores de redes**
  - **usuários**
- **A melhora não virá somente do uso de tecnologias de segurança ou da criação de leis**
  - **mas também da compreensão dos problemas e da mudança em como as pessoas usam e desenvolvem a tecnologia**

"The demands for the telegraph have been constantly increasing; they have been spread over every civilized country in the world, and have become, by usage, absolutely necessary for the well-being of society."

New York Times, April 3 1872

Fonte: "*The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*"

ISBN-13: 978-0802716040

Informações de Contato

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

Cristine Hoepers
cristine@cert.br