



egi
Escola de Governança
da Internet no Brasil

Fundamentos de Segurança da Internet

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

30/03/2016



Objetivos

Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência de sistemas conectados à Internet

De forma não exaustiva



Segurança e Governança da Internet



Cúpula Mundial Sobre a Sociedade da Informação: **Declaração de Princípios de Genebra**

12 de dezembro de 2003

[...]

B5) Promoção de confiança e segurança na utilização das TIC

35. O fortalecimento da estrutura de confiança, **incluindo segurança da informação e segurança das redes, autenticação, privacidade e proteção do consumidor**, é um pré-requisito para o desenvolvimento da Sociedade da Informação e para a promoção da confiança entre os usuários das TIC.

[...]

<http://cgi.br/publicacao/cadernos-cgi-br-documentos-cmsi/>



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: Princípios da Governança da Internet

Declaração Multissetorial do NETmundial

24 de abril de 2014

[...]

Segurança, estabilidade e resiliência da internet

A segurança, estabilidade e resiliência da Internet deve ser um objetivo fundamental de todos os atores da governança da Internet. Como um recurso global universal, a Internet deve ser uma rede **segura, estável, resiliente, confiável e fidedigna. A eficácia** no tratamento dos riscos e ameaças à segurança e estabilidade da Internet **depende de uma forte cooperação entre os diferentes atores.**

[...]

<http://cgi.br/publicacao/cadernos-cgi-br-declaracao-multissetorial-do-netmundial/>



Segurança da Informação



Propriedades da Segurança da Informação

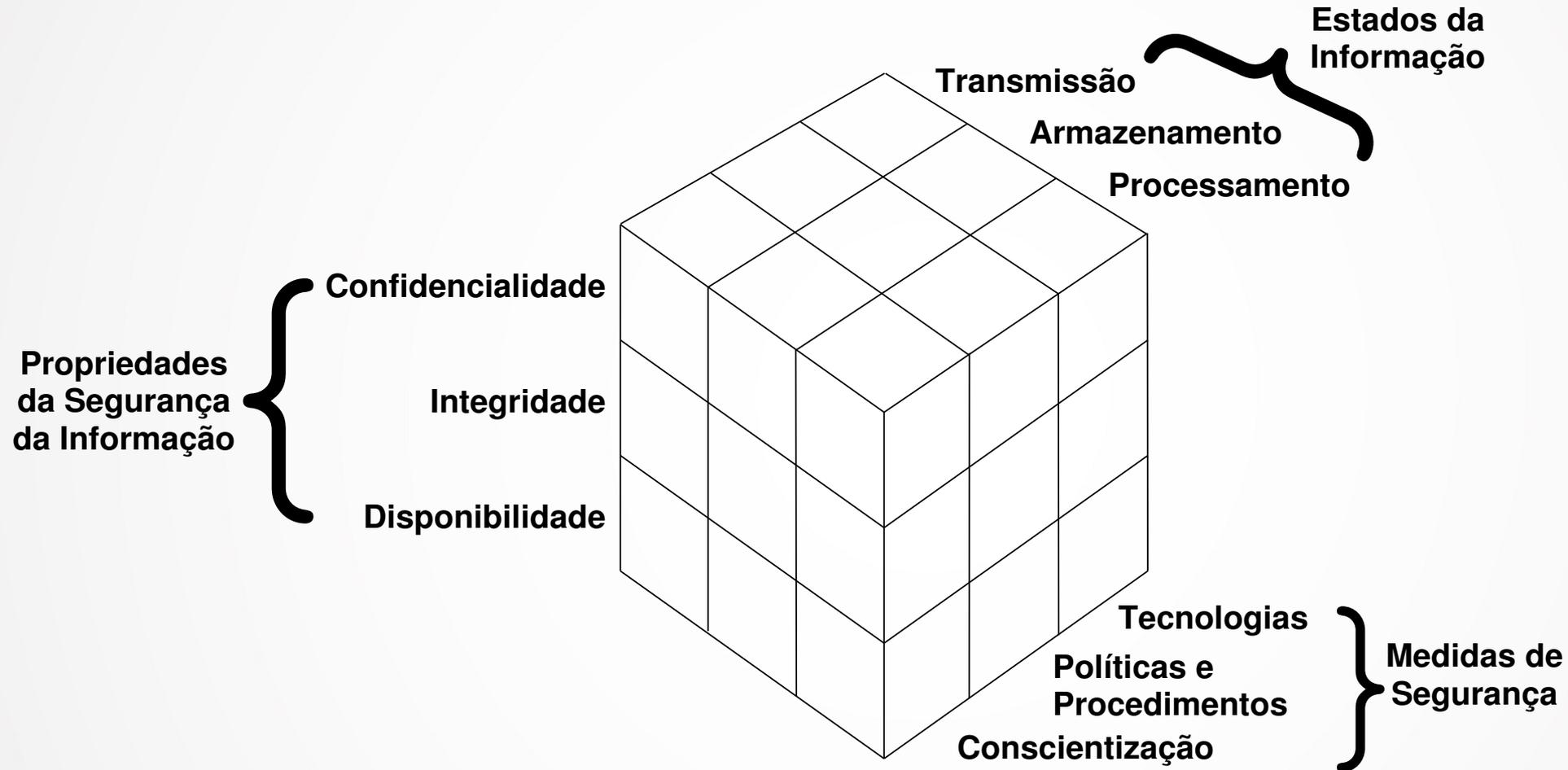
Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

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.



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/>

Privacidade vs. Confidencialidade

Do ponto de vista de Segurança da Informação:

Privacidade – habilidade e/ou direito de proteger suas informações pessoais, estende-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.



Riscos a 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

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas



Importância da Criptografia

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais
- mecanismos de autenticação
- conexão segura na Web (HTTPS)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC)



Registros de Eventos (*Logs*)

São os registros de atividades gerados por programas e serviços de:

- computadores (servidores e clientes);
- elementos de rede;
- dispositivos.

Seus formatos são definidos pelos desenvolvedores dos sistemas e aplicações

A partir da análise destas informações é possível:

- registrar as atividades normais;
- detectar problemas de *hardware* ou nos programas e serviços instalados no computador;
- detectar um ataque;
- detectar o uso indevido do sistema.



Exemplo de Registros de Eventos: **Logs de funcionamento 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/  
g27es04pw9re5ggrfp3suf8ew6t53asfz8/041-0925.English.d  
ist: Error Domain=NSXMLParserErrorDomain Code=4 "zero  
length data" UserInfo=0x7fed3da20e50  
{NSLocalizedString=zero length data}
```



Exemplo de Registros de Eventos: *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 17:40:20 notebook Firewall[65]: Stealth Mode connection
attempt to UDP 192.0.2.209:5060 from 199.19.109.76:5079
```



Exemplo de Registros de Eventos: *Logs de autenticação em uma conta de um sistema*

```
Mar 29 13:36:52 computador sshd[2540]: Accepted  
keyboard-interactive/pam for usuario from 192.0.2.68  
port 16608 ssh2
```

```
Mar 29 13:36:53 computador sshd: usuario [priv][2540]:  
USER_PROCESS: 2548 ttys001
```

```
Mar 29 13:42:14 computador sshd[2556]: Accepted  
keyboard-interactive/pam for usuario from  
2001:db8:0:2001::68 port 29580 ssh2
```

```
Mar 29 13:42:14 computador sshd: usuario [priv][2556]:  
USER_PROCESS: 2559 ttys001
```



Exemplo de Registros de Eventos: **Logs de conexão de um dispositivo a uma rede**

```
Mar 30 01:28:10 servidor dhcpd[154]: DHCPREQUEST for 10.0.0.165 from 74:81:14:xx:xx:xx via fxp1
```

```
Mar 30 01:28:10 servidor dhcpd[154]: DHCPACK on 10.0.0.165 to 74:81:14:xx:xx:xx via fxp1
```

Este é um exemplo dos dados de início de conexão, conforme definido no Marco Civil:

Art. 5º, VI - registro de conexão: o conjunto de informações referentes à **data e hora de início e término de uma conexão à internet**, sua duração e o **endereço IP utilizado pelo terminal** para o envio e recebimento de pacotes de dados;



Reflexões sobre *logs*

Não há padrão

- Cada serviço tem necessidades diferentes

Qualidade dos *logs*

- Horário sincronizado (NTP)
- Data completa, incluindo ano e fuso horário

Armazenamento de porta de origem

- A maior parte dos sistemas que rodam as aplicações na Internet não possui esse recurso
 - servidores Web
 - sistemas de balanceamento de carga
- Não é previsto como padrão nos protocolos (RFCs do IETF)
- Não será necessário em alguns anos



Obrigado

Cristine Hoepers, D.Sc.
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
jessen@cert.br

nic.br egi.br

www.nic.br | www.cgi.br