nic.br cgi.br | cert.br

Curso Livre: Estrutura e Funcionamento da Internet – aspectos técnicos, políticos e regulatórios

04 de novembro de 2020

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

Filiações e Parcerias:

Criação:

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos alocados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br).

Foco das Atividades

- Ponto de contato nacional
- Trabalho colaborativo com outras entidades
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

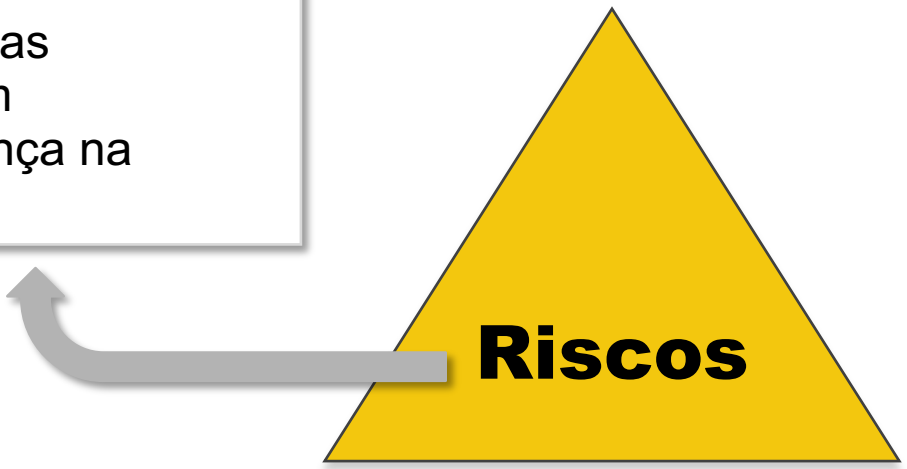
O Papel da Criptografia no Ecossistema da Internet

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

Riscos em Sistemas Conectados à Internet

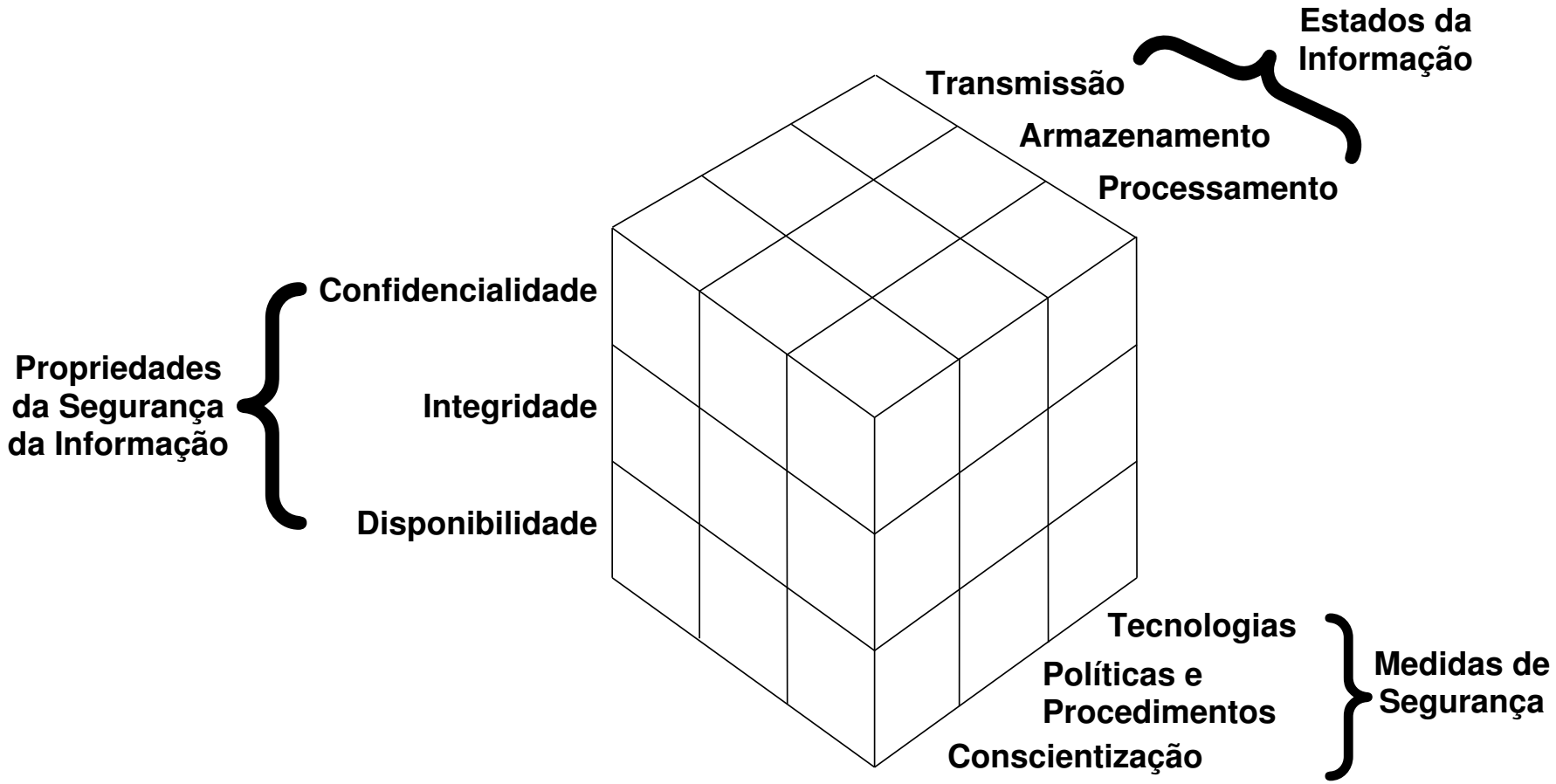
- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia



- criminosos
- espionagem industrial
- governos
- vândalos

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

Os dados e as informações estão em diversos locais e a segurança (proteção) depende de múltiplos fatores



McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

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.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

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.

Fonte: ***Security Engineering, 2nd Edition*****, 2008, Ross Anderson**
http://www.cl.cam.ac.uk/~rja14/book.html

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 (ex: atualização de *software* depende de assinaturas)
- mecanismos de autenticação (ex: acesso a contas de *e-mail* e redes sociais)
- conexão segura na Web (HTTPS)
  - confidencialidade
  - integridade (Estou conectando no *site* que eu realmente queria? O conteúdo não foi alterado no meio do caminho?)
- 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) e segurança de roteamento (RPKI)
- *blockchain*

Cartilha de Segurança para a Internet, Capítulo 9, ISBN: 978-85-60062-54-6 – https://cartilha.cert.br/livro/

Organizações Precisam Almejar Resiliência

Um sistema 100% seguro é muito difícil de atingir

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

- **Identificar o que é crítico** e precisa ser mais protegido (Análise de Risco)
- **Definir políticas** (de uso aceitável, acesso, segurança, etc)
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- **Implantar medidas de segurança** que implementem as políticas de segurança, como:
  - aplicar correções e instalar ferramentas de segurança
  - utilizar criptografia forte, que não dependa somente da segurança das chaves privadas – exemplo: ***Forward Secrecy*** (protege transações passadas contra um comprometimento ou espionagem)
- Formular **estratégias e processos para gestão de incidentes** de segurança e formalizar **grupos de tratamento de incidentes (CSIRTs)**

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br