

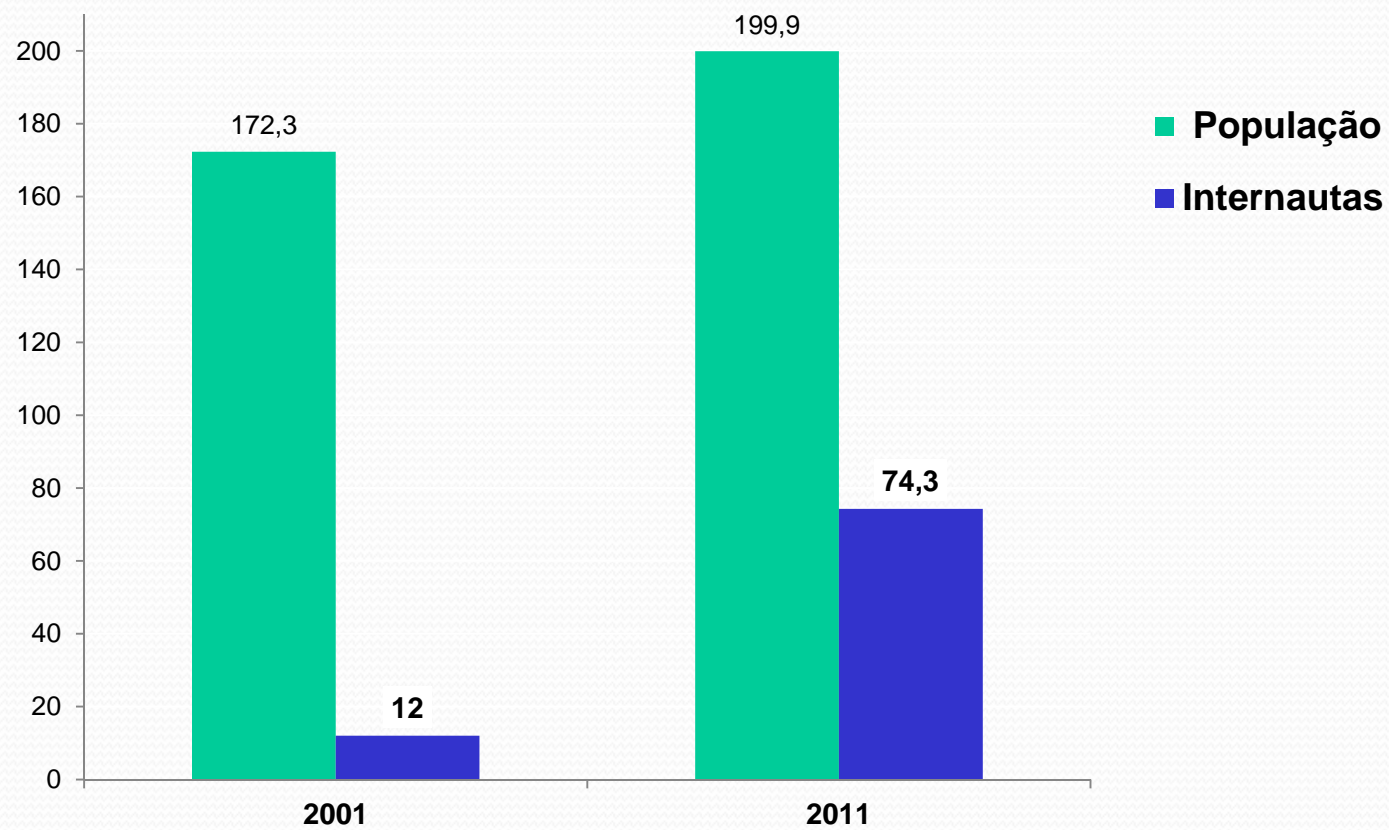
Segurança e Certificados Digitais

E-commerce

Professor Fabiano Santos de Oliveira
Faculdade Alfa de Umuarama

Motivação

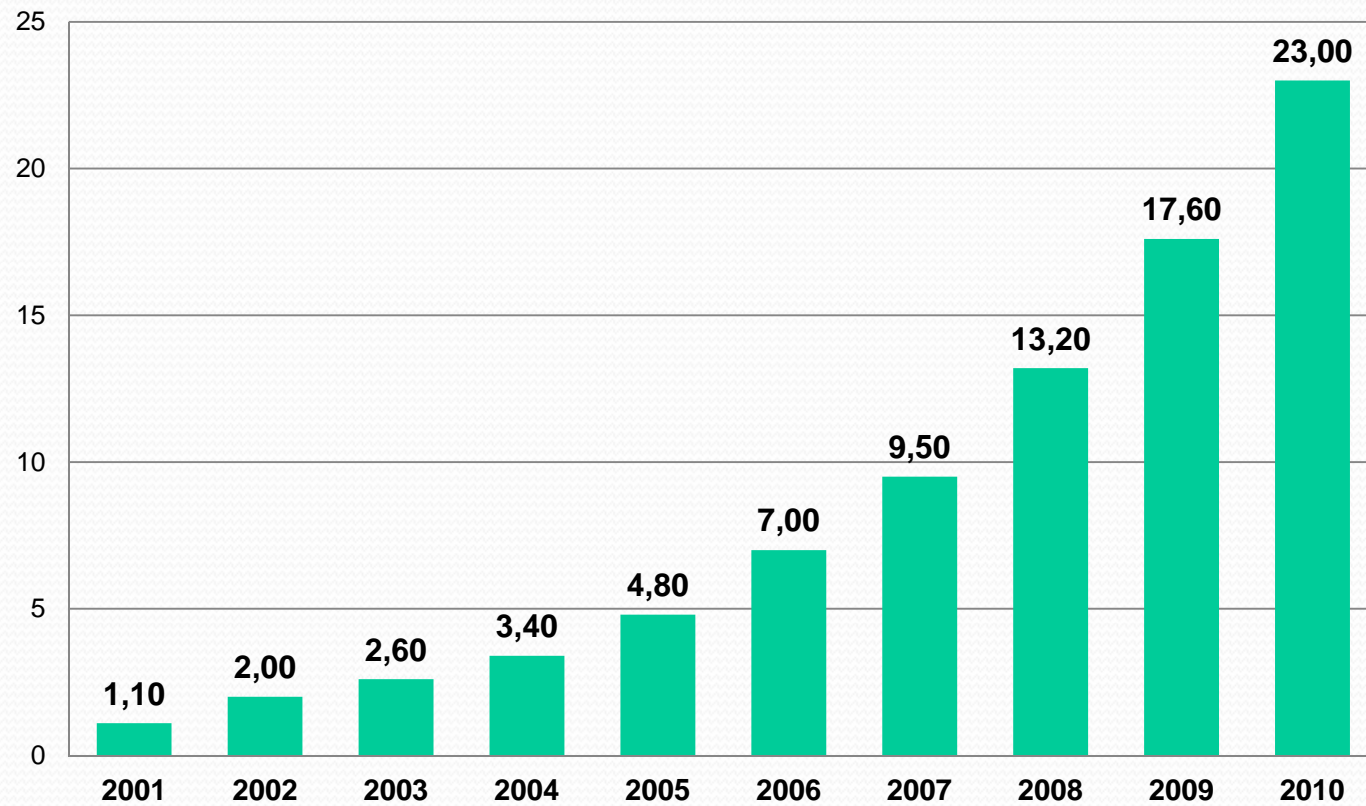
Projeção de Crescimento da Internet
no Brasil (em milhões)



Fonte: eBit - Compilação www.e-commerce.org.br

Motivação

Quantidade de e-consumidores no Brasil (em milhões)

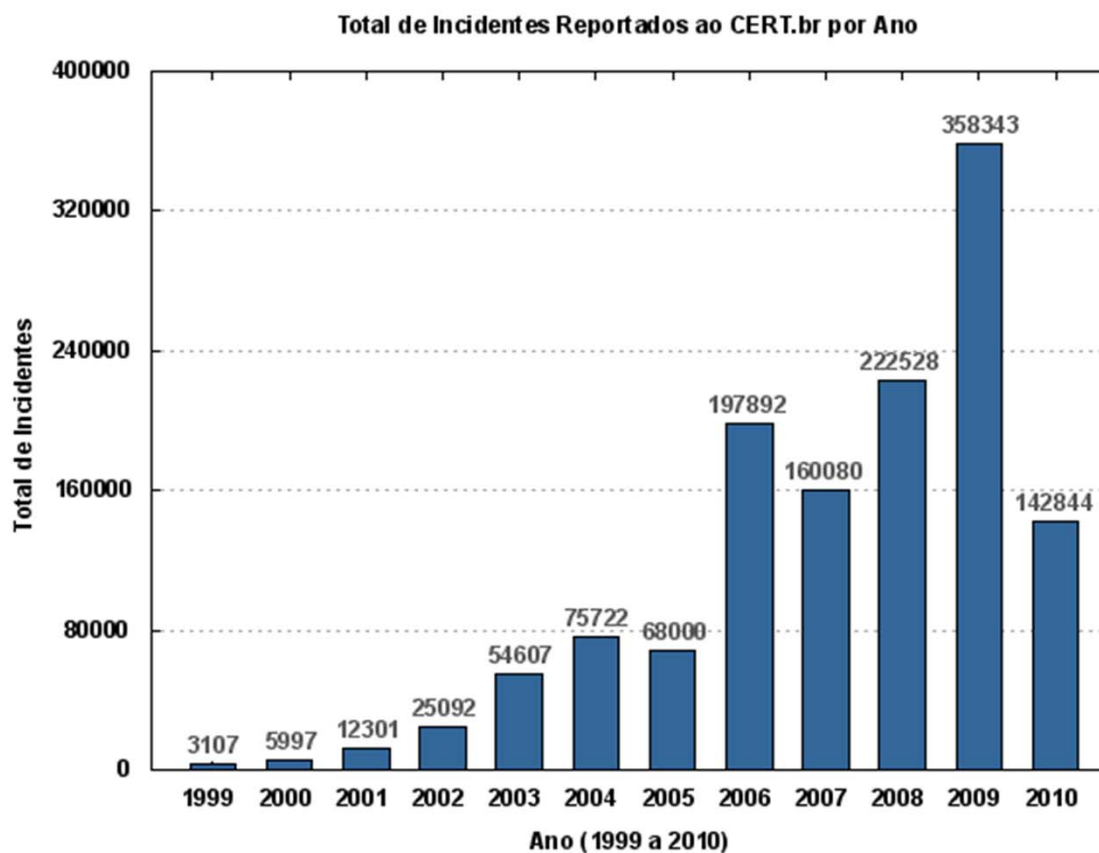


Fonte: eBit - Compilação www.e-commerce.org.br

Motivação

| 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999 |

Valores acumulados: 1999 a 2010 **novo**



Fonte: www.cert.br

Sobre o CERT

- O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.
- É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.
- Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.



A Internet

- Segurança da informação sempre foi uma preocupação (criptografia).
- [?] Aumento da utilização do meio eletrônico para transações sigilosas.
- [?] Comércio Eletrônico, e-mail seguro, troca de documentos em geral.

Fato

A Internet **NÃO** é segura!!

**Como garantir a
segurança?**



Certificação Digital

- Tecnologia de identificação.
- Mecanismos que evitam:
 - **adulterações, interceptações** ou outros tipos de **fraudes**.
- Capazes de garantir:
 - **autenticidade, confidencialidade e integridade**.
- Atribuição de responsabilidade: **não-repúdio** à operação.
 - O emissor não pode negar a autoria da mensagem.

Certificação Digital

Como funciona?

Se baseia num documento eletrônico chamado **certificado digital** e no recurso de **assinatura digital**.



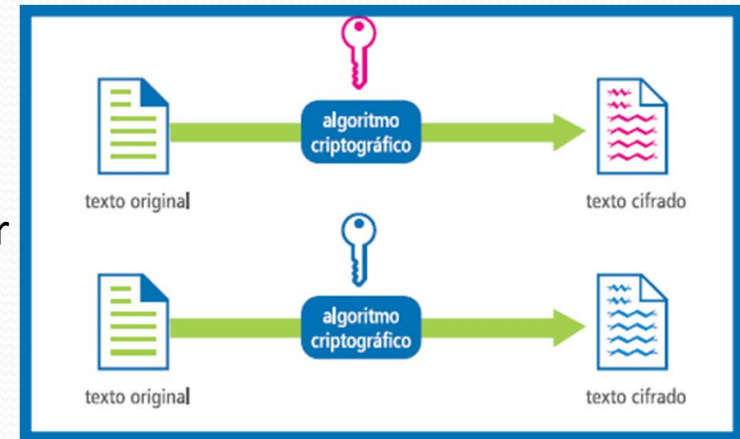
Certificado Digital

- Documento eletrônico que identifica pessoas físicas e jurídicas e também servidores.



Criptografia

- Arte de escrever em códigos.
- Envolve 2 processos: **cifragem** e **decifragem**.
- Usa **chaves criptográficas** – sem o conhecimento da chave correta não é possível decifrar um texto cifrado.



O certificado digital é emitido a:

- ✓ Pessoas Físicas (cidadão comum)
- ✓ Pessoas Jurídicas (empresas ou municípios)
- ✓ Equipamentos
- ✓ Aplicações



Certificado Digital

Como solicitar?

-Autoridade Certificadora.



ICP-BRASIL



- ✓ Infra-estrutura de chaves públicas brasileira.
- ✓ Estabelece os fundamentos **técnicos** e **metodológicos** para uso de chaves públicas.
- ✓ **Padronizou**, e mantém as **regras** do uso de chaves no país.
- ✓ Administrado pelo **ITI** - Instituto Nacional de Tecnologia da Informação
- ✓ Medida Provisória 2.200-2 de 2001.



INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Autoridades Certificadoras



