

## O QUE É SEGURANÇA DA INFORMAÇÃO?

- Processo de proteção das **informações** e **ativos digitais** armazenados em computadores e redes de processamento de dados.



## QUAIS INFORMAÇÕES PROTEGER?

- Identidade, CPF
- Endereço residencial
- Telefone celular
- Senha da agenda eletrônica
- Informações bancárias e senhas
- Senhas de acesso da empresa
- Número do Cartão de Crédito
- Etc.



## POR QUE PROTEGER?

- Por seu valor
- Pelo impacto da ausência
- Pelo impacto pelo uso de terceiros
- Pela importância de sua existência
- Pela relação de dependência com suas atividades.



## QUANDO PROTEGER

- Durante o ciclo de vida da informação.
  - Manuseio
  - Armazenamento
  - Transporte
  - Descarte



## ATIVOS

- Elementos aos quais a organização atribui **valor** e portanto requerem proteção.

## ATIVOS

- Exemplos:
  - Informações impressas ou digitais
  - Hardware
  - Imagem de um Empresa
  - Confiabilidade de um Órgão Federal
  - Marca de um Produto

ATIVOS	FÍSICOS	TECNOLÓGICAS	HUMANOS
	<ul style="list-style-type: none"><li>• agenda</li><li>• sala</li><li>• arquivo</li><li>• cofre</li></ul>	<ul style="list-style-type: none"><li>• sistema</li><li>• e-mail</li><li>• servidor</li><li>• notebook</li></ul>	<ul style="list-style-type: none"><li>• funcionário</li><li>• parceiro</li><li>• secretária</li><li>• porteiro</li></ul>

## PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO


- **Confidencialidade**

- proteger informações confidenciais contra revelação não autorizada ou captação compreensível;

- **Integridade**

- Toda informação deve ser protegida afim de se evitar que dados sejam apagados ou alterados de alguma forma não autorizada.

- **Disponibilidade**


- Toda informação deve ser protegida afim de que os serviços de informática não sejam degradados ou tornados indisponíveis.
- 

## ASPECTOS DA SEGURANÇA


- **Autenticação**

- Processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica.


- **Legalidade**

- característica das informações que possuem valor legal dentro de um processo de comunicação, estando de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
- 

## CIDAL

- C – Confidencialidade
  - I – Integridade
  - D – Disponibilidade
  - A – Autenticação
  - L - Legalidade
- 

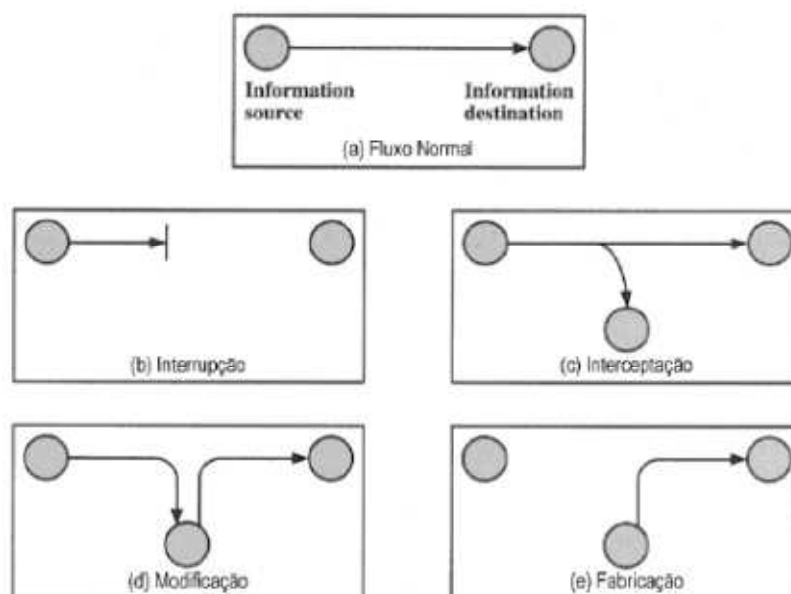
## AMEAÇAS

- Ameaças são causas potenciais de incidentes não esperados, os quais talvez resultem em danos para aos ativos da organização. Exploram falhas de segurança.
- 

## TIPOS DE AMEAÇAS

- **Naturais:** Fenômenos da natureza.
  - Incêndios, enchentes, terremotos, maremotos, aquecimento, poluição, etc.
- **Intencionais:** propositais
  - Hackers, ladrões, programas que executam códigos maliciosos (malwares).
- **Involuntárias:** Perigos trazidos pela ignorância por usuários não treinados ou falta de atenção.

## AMEAÇAS E ATAQUES



## AMEAÇAS E ATAQUES

- Ataques sobre o fluxo de informação
  - **Interrupção**: ataca a disponibilidade
  - **Interceptação**: ataca a confidencialidade
  - **Modificação**: ataca a integridade
  - **Fabricação**: ataca a autenticidade




## VULNERABILIDADES

- **Fragilidade** presente ou associada a ativos que manipulam e/ou processam informações que, ao ser **explorada por ameaças**, permite a ocorrência de um **incidente de segurança**, afetando negativamente um ou mais **princípios da segurança da informação**.






## TIPOS DE VULNERABILIDADES

- **Físicas**
    - Salas do CPD mal planejadas, falta de extintores, vazamentos, instalações fora do padrão.
  - **Naturais**
    - Incêndios, enchentes, terremotos, tempestades, falta de energia, acúmulo de poeira, etc.
  - **Hardware**
    - Desgaste, má utilização, falha nos recurso tecnológicos, etc.
- 

## TIPOS DE VULNERABILIDADES

- **Software**
    - Erros de configuração, erros de instalação, perda de dados, indisponibilidade de recursos.
  - **Mídia**
    - Discos, fitas, relatórios e impressos podem ser perdidos ou danificados.
  - **Comunicação**
    - Acessos não autorizados ou perda da comunicação.
- 

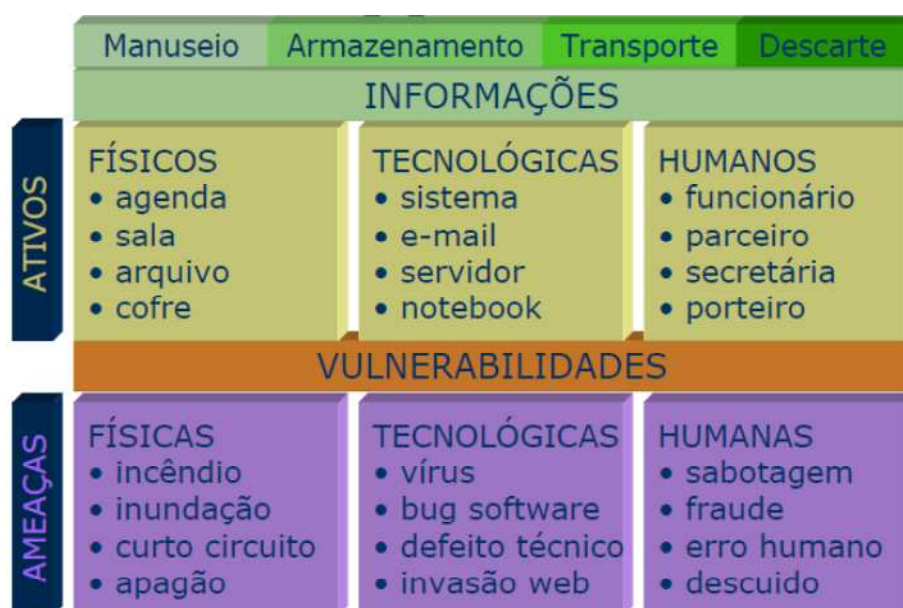
## TIPOS DE VULNERABILIDADE

- **Humanas**

- Falta de treinamento, erros ou omissões, sabotagens, greve, vandalismo, roubo, etc.



## EM RESUMO...



## IMPACTO

**Abrangência** dos danos causados por um **incidente de segurança** sobre um ou mais **processo de negócio**.



## RISCOS

- Probabilidade de ameaças **explorarem vulnerabilidades**, provocando perdas de confidencialidade, integridade e disponibilidade, causando possivelmente, **impactos nos negócios**.

$$\text{R} = \frac{\text{Ameaças} \times \text{Vulnerab.} \times \text{Impactos}}{\text{Medidas de Segurança}}$$

risco

## RISCO

○ **AMEAÇAS** exploram  
**VULNERABILIDADES**  
presentes nos **ATIVOS** que  
mantém informações, causando  
**IMPACTOS** no Negócio



## MEDIDAS DE SEGURANÇA

São as **práticas**, os **procedimentos** e os **mecanismos**  
usados para a proteção da informação e seus ativos, que  
podem impedir que ameaças explorem  
vulnerabilidades.



## MEDIDAS DE SEGURANÇA

- Preventivas
- Corretivas
- Detectáveis



## MEDIDAS DE SEGURANÇA PREVENTIVAS

- Tem como objetivo de evitar que incidentes venham a ocorrer.
  - Políticas de Segurança; instruções e procedimentos de trabalho; campanhas e palestras de conscientização de usuários; ferramentas como firewall, antivírus, etc



## MEDIDAS DE SEGURANÇA DETECTÁVEIS

- Visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades.
  - análise de riscos; sistemas de detecção de intrusão; alertas de segurança; câmeras de vigilância, alarmes, etc...



## MEDIDAS DE SEGURANÇA CORRETIVAS

- Correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos;
  - equipes para emergências, restauração de backup; plano de continuidade operacional; plano de recuperação de desastres; etc

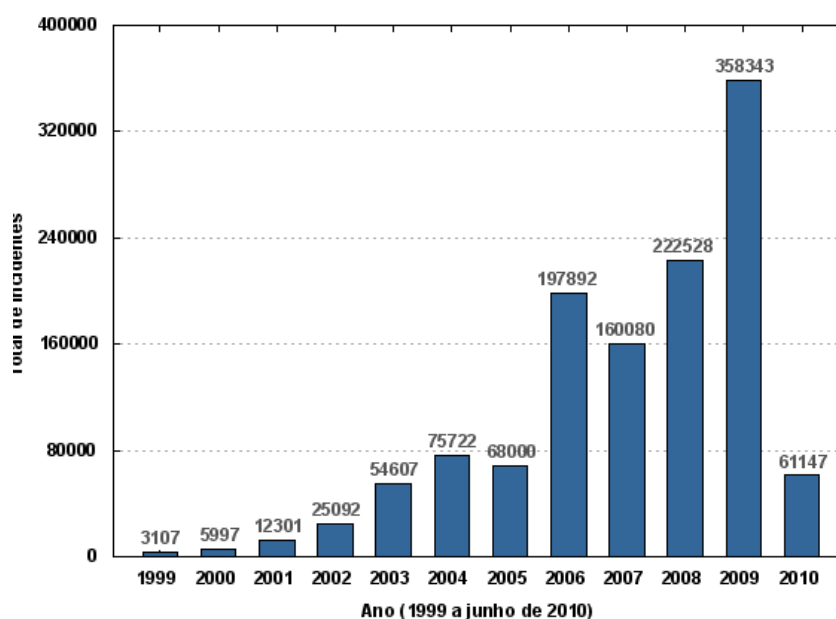


## NO BRASIL: CERT.BR

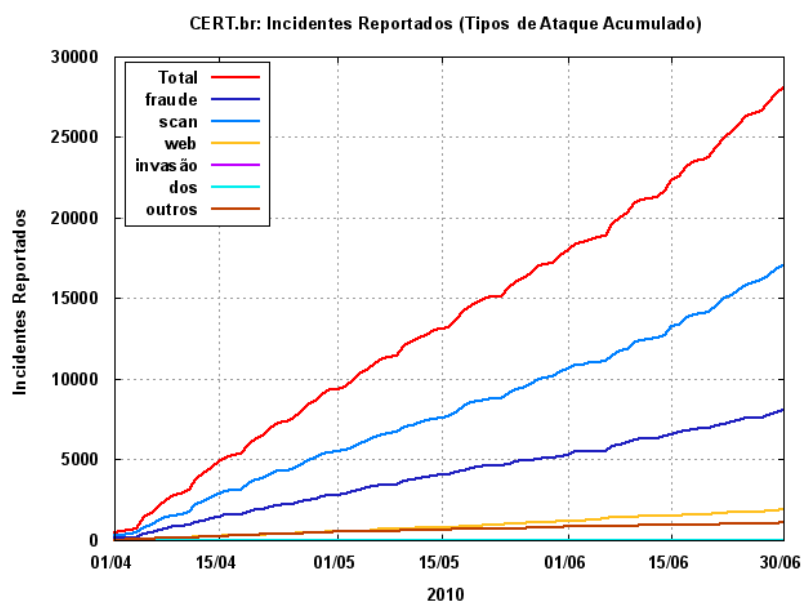
- Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil
- Mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.
- Atua como um ponto central para notificações de incidentes de segurança no Brasil.
- Coordena e o apóia no processo de resposta a incidentes.
- Trabalho de conscientização sobre os problemas de segurança e análise de tendências.

## ALGUMAS ESTATÍSTICAS DO CERT.BR

Total de Incidentes Reportados ao CERT.br por Ano



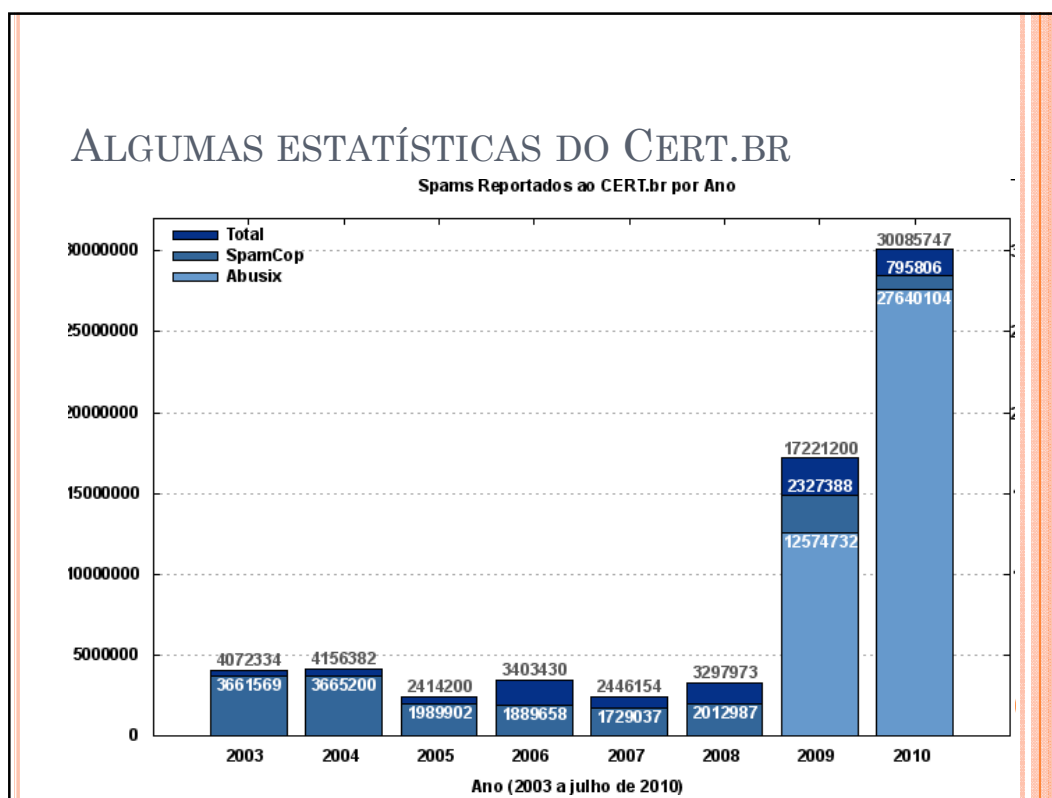
## ALGUMAS ESTATÍSTICAS DO CERT.BR



## ALGUMAS ESTATÍSTICAS DO CERT.BR







## VÍDEO

- Navegar é preciso. CGI.Br



## REFERÊNCIAS

- Sêmola, Marcos. A Importância da Gestão da Segurança da Informação. Slides.
- <http://www.cert.br/>
- Guia de Referência Sobre Ataques Via Internet. Febraban. 2000.

