Conceitos de segurança em SI

Roteiro

- Entender o **conceito de segurança em SI**
  - Definição
  - Focos de preocupação
- Discutir quais são as principais "**áreas de vulnerabilidade**" em SI
  - discussão "tradicional": 5 áreas de vulnerabilidade
  - visão "complementar": 3 camadas de segurança

O que é segurança em SI

Segundo a Norma ISO/IEC 17799: 2000 *
(atualmente ISO/IEC 27002: 2007)

… ***preservação de três <u>atributos básicos da informação</u>:***

- *integridade*
- *confidencialidade*
- *disponibilidade*

* IEC – International Electrotechnincal Commission (www.iec.ch)

Atributos de um sistema seguro

- Integridade
  - Garantir a não alteração de dados em transmissão ou armazenados
- Confidencialidade
  - Garantir que os dados não sejam acessados por não autorizados
- Privacidade
  - Garantir que os dados não sejam revelados/fornecidos indevidamente
- Disponibilidade
  - Garantir que o recurso esteja disponível quando necessário
- Autenticidade
  - Garantir que o executor de uma ação seja mesmo quem ele alega ser
- Não-repudiação
  - Garantir que o executor de uma ação não possa negar tê-la feito

Fontes de problemas: 5 “áreas de vulnerabilidade” de SI

Desastre

Risco de hardware ou arquivos de dados poderem ser destruídos (incêndios, enchentes, problemas na rede elétrica, etc.)

Invasão

Acesso não-autorizado (alterações, roubo ou danos físicos)

Erros e Bugs

Falhas no ciclo de desenvolvimento do sistema

Defeitos no código do programa

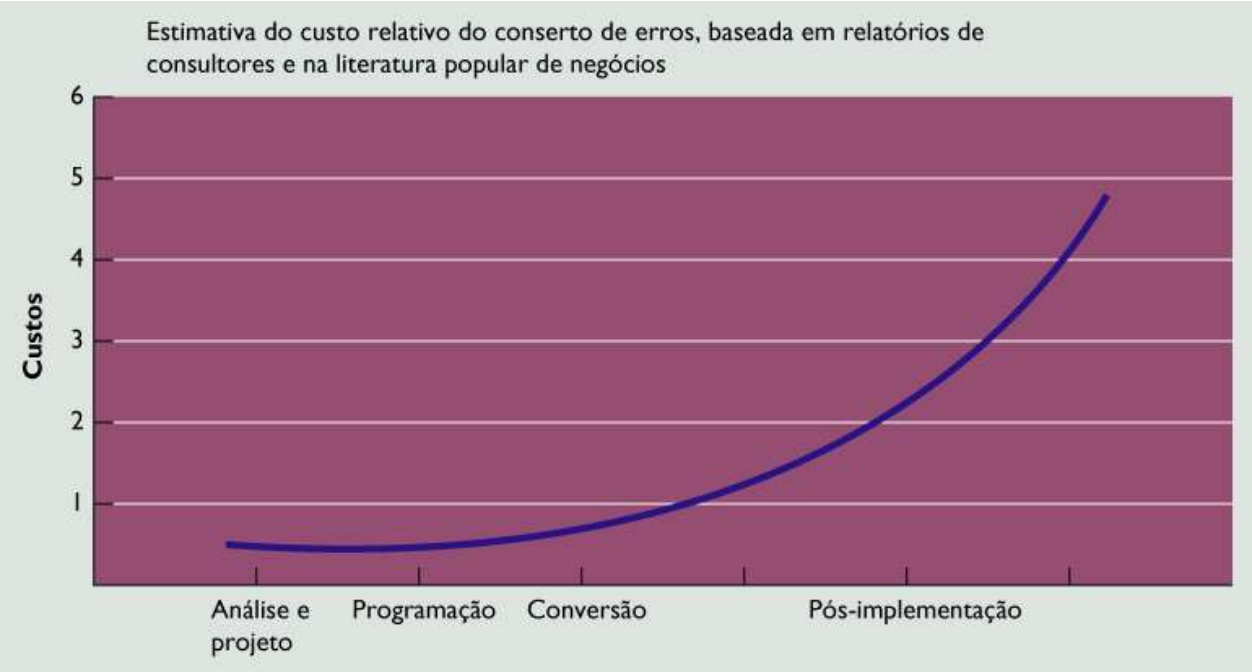
Qualidade dos dados

Causados por problemas durante a entrada de dados ou no projeto do sistema de informação e do banco de dados

Manutenção

Alto custo de correção de falhas na análise e no projeto de sistemas

Custo dos erros no ciclo de desenvolvimento de sistemas



Fontes de problemas:
3 “Camadas” da segurança em SI

Camada física

- espaço físico onde o hardware está instalado;
- equipamentos;
- controle de acesso físico
- no breaks, climatização
- o meio de comunicação em si

Camada lógica

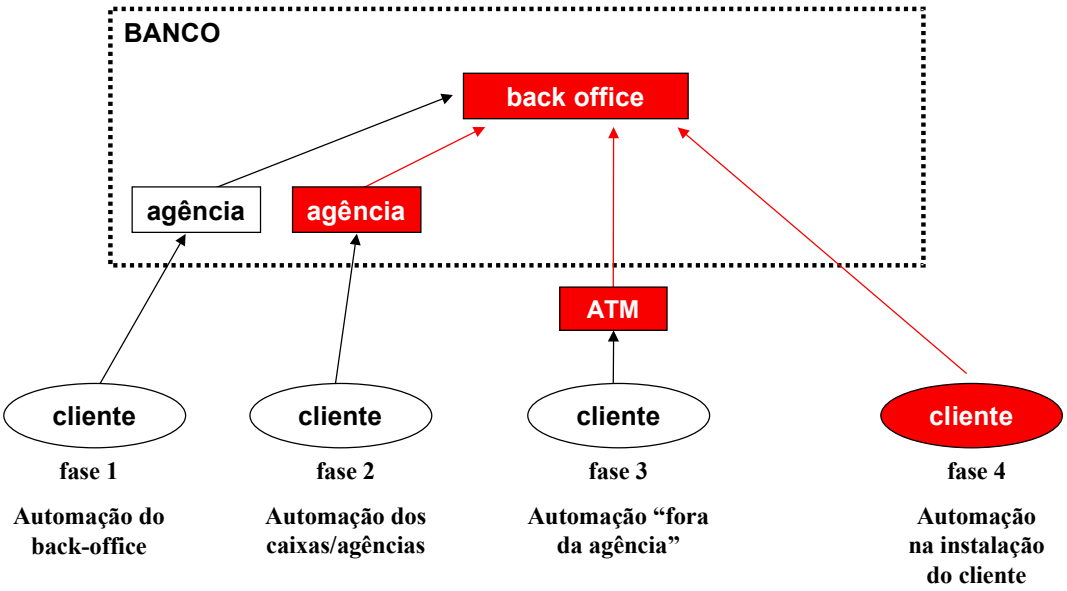
- os *softwares;* encriptação e decriptação; antivírus, etc.

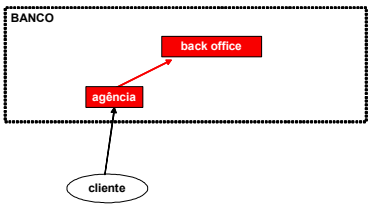
Camada humana

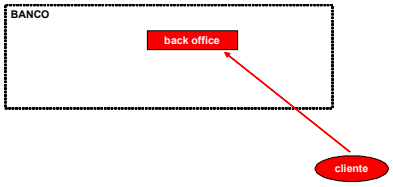
- recursos humanos envolvidos; elo mais fraco na corrente da segurança;
- conscientização, conhecimento das políticas de segurança;
- percepção do risco pelas pessoas: como lidam com os sinistros que ocorrem raramente;
- o perigo dos intrusos maliciosos ou ingênuos; a engenharia social onde *hackers* conseguem informações por lícitos.

COMO A EVOLUÇÃO DO USO DE TI TEM AUMENTADO O RISCO DAS EMPRESAS EM CADA UMA DAS 3 CAMADAS ?

Exemplo para discussão:
fases do uso de SI *versus* segurança em transações bancárias







Camada Física
- Restrita ao ambiente controlado pelo banco
- Rede privada
- Fechada no ambiente interno
- Restrito ao espaço do banco

Camada Lógica
- Tráfego interno
- Aplicativos próprios

Camada Humana
- Restrita, controlada
- Treinada

Camada Física
- Acesso público e irrestrito
- Rede pública
- Aberta e global
- Espaço múltiplo: domicílio do cliente, cibercafé, etc.

Camada Lógica
- Uso intenso de tráfego externo
- Aplicativos de mercado

Camada Humana
- Ampliada, pouco controle
- Heterogênea

Roteiro

- Entender o **conceito de segurança em SI**
  - Definição
  - Focos de preocupação

- Discutir quais são as principais "**áreas de vulnerabilidade**" em SI
  - discussão "tradicional"
  - visão "complementar"