PUC Minas

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Aluno: André Luiz Dias Etapa 4

Cartilha Básica de Segurança da Informação

- Hoje em dia a informação é o bem mais valioso de uma empresa/Cliente.

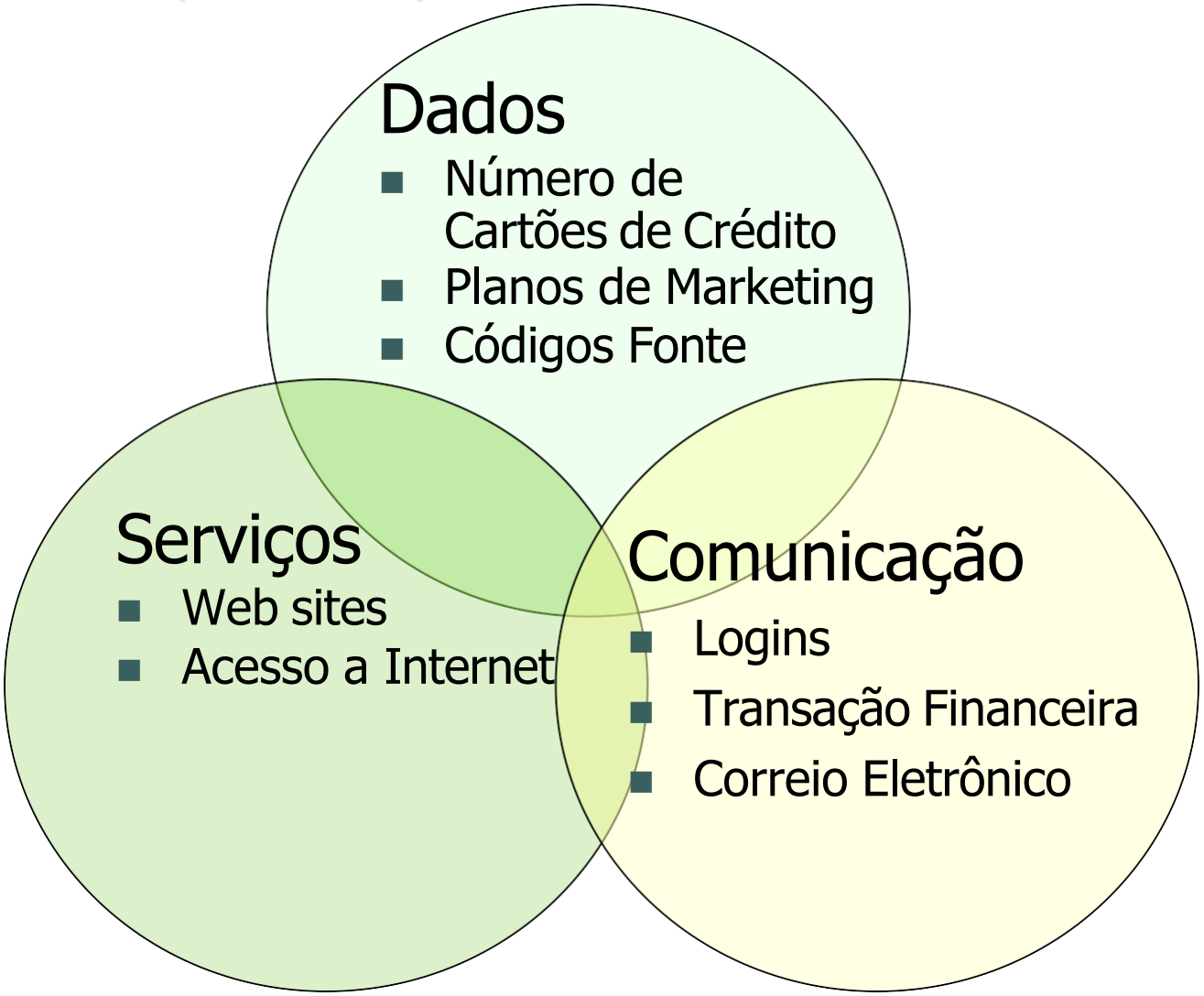
Segurança da Informação

- “A segurança da informação é um conjunto de medidas que se constituem basicamente de **controles** e **política de segurança**, tendo como objetivo a proteção das informações dos clientes e da empresa (**ativos/bens**), controlando o **risco** de revelação ou alteração por pessoas não autorizadas.”

Política de Segurança

- Trata-se um conjunto de diretrizes (normas) que definem formalmente as regras e os direitos dos usuários, visando à proteção adequada dos ativos da informação.

Ativos (Bens)


Dados
Número de Cartões de Crédito
Planos de Marketing
Códigos Fonte
Serviços
Web sites
Acesso a Internet
Comunicação
Logins
Transação Financeira
Correio Eletrônico

Definições

- Ameaça
  - Evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um recurso;
- Vulnerabilidade
  - Característica de fraqueza de um bem;
  - Características de modificação e de captação de que podem ser alvos os bens, ativos, ou recursos intangíveis de informática, respectivamente, software, ou programas de bancos de dados, ou informações, ou ainda a imagem corporativa.

Definições

- Risco
  - A **probabilidade** da ocorrência de uma ameaça em particular
  - A **probabilidade** que uma ameaça explore uma determinada vulnerabilidade de um recurso

Princípios da Politica de Segurança

- Integridade
  - Condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas
- Confidencialidade
  - Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono
- Disponibilidade
  - Possibilidade de acesso à informação por parte daqueles que a necessitam para o desenvolvimento de suas atividades

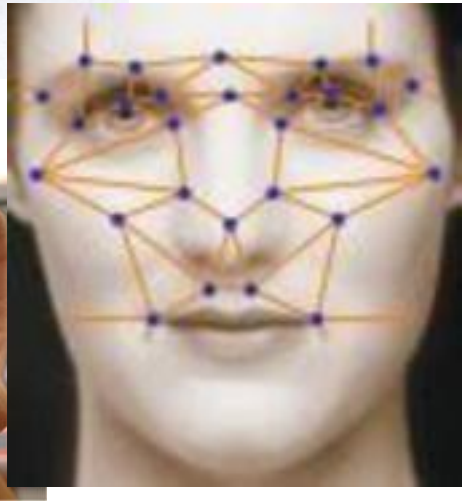
Ameaças à Politica de Segurança

- Integridade
  - Ameaças de ambiente (fogo, enchente...), erros humanos, fraudes, erro de processamento
- Divulgação da informação
  - Divulgação premeditada ou acidental de informação confidencial
- Indisponibilidade
  - Falhas de sistemas

Mecanismos de segurança

- Controle físico
  - Barreiras que limitam o contato ou acesso direto à informação ou a estrutura que a suporta
    - Porta, paredes, trancas, blindagem, guardas ...
- Controle lógico
  - Barreiras que limita o acesso à informação em ambiente eletrônico
    - Mecanismos de criptografia
      - Modificar a informação de forma que seja impossível que pessoas não autorizadas a decodifiquem
    - Mecanismos de controle de acesso
      - Senhas, Firewall, Sistemas biométricos

Mecanismos de Controle de Acesso



Vírus de Computador

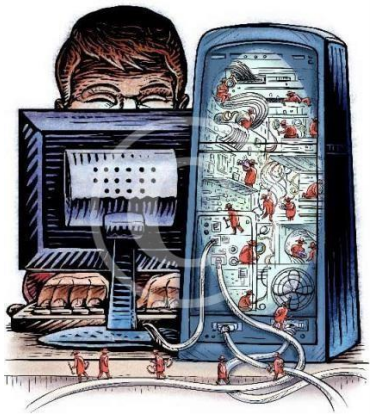
- São programas criados para causar danos ao computador:
  - Apagando dados
  - Capturando informações
  - Alterando o funcionamento normal da máquina
- Tipos de vírus
  - Worm: Tem o objetivo principal de se espalhar o máximo possível, não causando grandes danos

Vírus de Computador

- Trojan ou Cavalo de Troia: Permite que outra pessoa tenha acesso ao computador infectado
  - Permite ao atacante enviar comandos a outro computador
  - Instalado quando o usuário “baixa” algum arquivo da Internet e o executa
  - Atualmente os Trojans são mais utilizados para roubar senha de bancos – Phishing

Vírus de Computador

- Spyware
  - Utilizado para espionar a atividade do computador afetado e capturar informações
  - Geralmente são embutidos em programas freeware ou shareware
- Keylogger
  - Tem a função de capturar tudo que é digitado pelo usuário do computador atacado



Vírus de Computador

- Hijacker: “Sequestram” o navegador de internet, alterando paginas, exibindo propagandas em pop-up, instalando barras de ferramentas

- Rootkit: Podem ser utilizados para várias finalidades, roubar senha, controlar o computador a distância, entre outros.
  - Detectar este problema é difícil pois ele se camufla no sistema, se passando por programas do sistema

Ferramentas de Proteção

- Antivírus
  - Procura por “assinatura” do vírus
  - Mais comuns:
    - AVG
    - Avast
    - Norton
    - Kaspersky
    - McAfee
- Firewall
  - Permitir a entrada de dados da rede para o computador, apenas de locais conhecidos

Política de Backup

Por que Fazer Backup?

Os dados contidos no disco rígido podem sofrer danos e ficar inutilizados por vários motivos

Exemplos de danos em arquivos: choque do disco, vírus, defeito no hardware ou eliminação acidental

Estratégias de Backup:

Cópias incrementais: cópia dos arquivos que foram criados ou modificados desde o último backup

Cópias completas: cópia de todos os arquivos, quer ele tenha sido alterado ou não

Organização de Pastas e Arquivos

Facilita o gerenciamento do backup

Exemplo: separação de arquivos por aplicativos, por projeto, por clientes, por fornecedores etc

Segurança Externa do Backup

- Armazenar em local protegido da umidade, mofo e incêndio
- Se o dado é de vital importância ter mais de uma cópia em locais diferentes
- Manter rótulo nos backup para facilitar a identificação
- Colocar em local de acesso restrito

Backup na Prática

Defina o grupo de arquivos que farão parte do backup

Estabeleça uma rotina a ser seguida pelo usuário.

Não espere acontecer para entender a importância de uma cópia de segurança (backup)

Dicas de Seguranças

- Saia de sites com autenticação utilizando o botão Sair, Logout ...
- Crie senhas difíceis
- Mude a senha periodicamente
- Atualize o seu navegador
- Fique atento ao realizar downloads
- Cuidado com links nos programas de mensagens instantâneas
- Cuidado com E-Mails falsos
- Atualize sempre o antivírus
- Atualize o sistema operacional
- Realize Backups periodicamente