Introdução à Segurança da Informação

ISO/IEC 27000

Prof. Marcos Argachoy

Segurança da informação

Conceitos

- **Segurança** é a minimização do risco associado às atividades de computação, incluindo a interconexão entre computadores e demais aspectos físicos e humanos.
- **Política de segurança** define controles lógicos e físicos assegurando um determinado nível de disponibilidade dos sistemas, confiabilidade dos dados e serve de referência para as ações de treinamento dos usuários e demais procedimentos de segurança.
- Não existe segurança ABSOLUTA.

Segurança da informação

Ameaças à Segurança

- Danos materiais;
- Vazamento de informações;
- Violação da integridade;
- Uso indevido;
- Interceptação de informações;
- Interrupção do serviço.

Segurança da informação

Conceitos

- **Ataque Passivo:** Apenas observa (coleta) informações.

  Exame de conteúdo, “sniffer”, análise de tráfego, etc...

- **Ataque Ativo:** podem alterar os dados ou informações.

  Repetição, Modificação de conteúdo de mensagens, “Man-in-the-middle”, simulação de incidente, negação de serviço.

Segurança da informação

Conceitos

Tipos de Ataque:

- Interrupção;
- Interceptação;
- Modificação;
- fabricação;

Segurança da informação

- Elementos de Segurança
  - Segurança física
    - **Instalações;** Antigas, inadequadas, sujeira, calor, fogo, rede elétrica, etc.
    - **Dados**; Bugs, previlégios, SW mal configurados, documentos impressos, CDs e outras mídias, “arquivo morto”, controle de versões, etc.

Segurança da informação

- Elementos de Segurança
  - Segurança de acesso
    - **Físico e Lógico;** Monitoração, controle e registro de acesso, senhas, teclado variável, identificação biométrica, Smart Cards, Dupla identificação (algo que o usuário sabe + algo que o usuário possui), TOKENs, etc.

Segurança da informação

Conceitos

Serviços de Segurança

- **Confidencialidade:** Garantir que a informação não será objeto de ataques passivos.
- **Autenticação:** Garantir que a origem e o destino das mensagens é o pretendido.
- **Integridade:** Garantia de que as mensagens não são alteradas, duplicadas, repetidas ou com a ordem alterada.
- **Não Repudiação:** Garantia que o autor não irá negar, no futuro, ter sido seu autor.

Segurança da informação

Conceitos

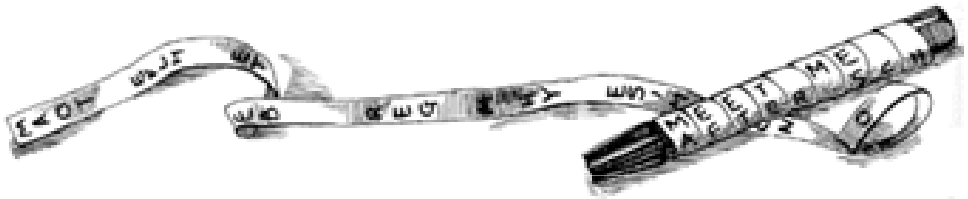
Mecanismos básicos de segurança

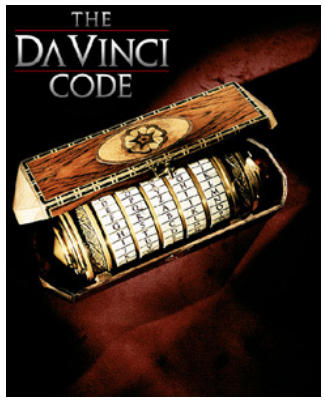
- **Criptografia:** É usada principalmente para garantir a confidencialidade. (existe também uma variante chamada **Esteganografia**)
- **Assinatura Digital:** Usadas para garantir a autenticidade, integridade e a não repudiação (e-CPF é um exemplo).
- **Checksums** / **hash:** Usados para garantir integridade (digito de controle do CPF, RG, etc.).

Segurança da informação

Criptografia primitiva

Cítala Espartana, utilizada em 480 AC





A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Cifra de César

Esta cifra foi utilizada pelos oficiais sulistas na Guerra de Secessão americana e pelo exército russo em 1915.

Segurança da informação

- Exemplo de Esteganografia:

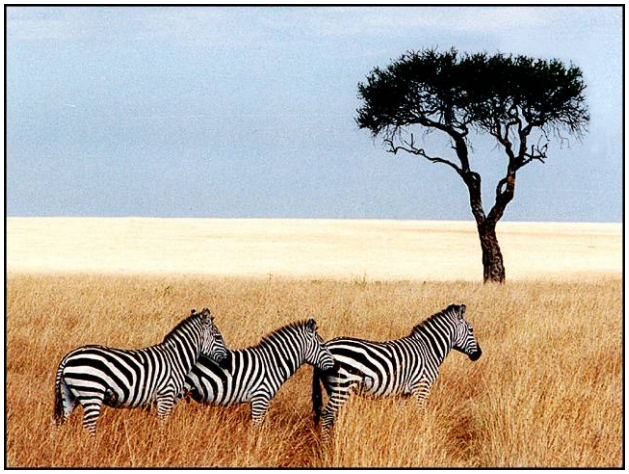


Foto comum

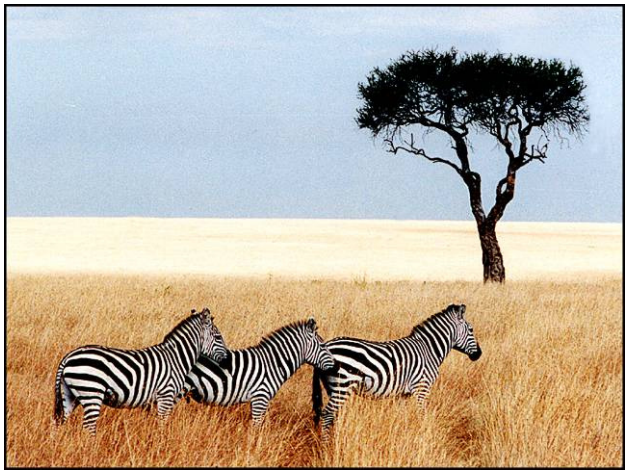


Foto +

5 obras de Shakespeare

Segurança da informação

- Exemplo de Esteganografia

Foto comum

Foto +

Apostila de Segurança

Segurança da informação

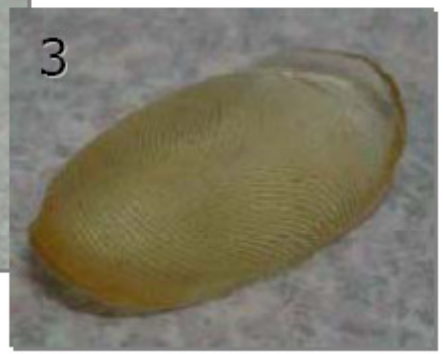
- Exemplo “falsificação” de impressão digital:

Funcionou em 80% das tentativas

Plástico moldável

Gelatina a 50%

“dedo” falso



Segurança da informação

ISO 27000

- Padrão aprovado em 2000 (USA);
- Baseada na BS 7799 (Norma Britânica bem mais antiga);
- É a referência para políticas e normas de segurança das empresas;
- Equivalente brasileira é a BR17799 aprovada em setembro de 2001;
- Evolução para a série 27000 em 2005;
- ISO/IEC 27000:2009 publicada em 30/04/2009;
- ISMS - Information Security Management System

Segurança da informação

ISMS

Information **S**ecurity **M**anagement **S**ystem,

Um sistema de gerenciamento de Segurança da Informação é formado por políticas, procedimentos, roteiros, recursos e atividades associadas, gerenciados em conjunto com uma organização com o objetivo de proteger os ativos de informação.

Segurança da informação

– **ISO/IEC 27000:2009**, Information security management systems — Overview and vocabulary

– **ISO/IEC 27001:2005**, Information security management systems — Requirements

– **ISO/IEC 27002:2005**, Code of practice for information security management

– **ISO/IEC 27003**, Information security management system implementation guidance

– **ISO/IEC 27004**, Information security management — Measurement

– **ISO/IEC 27005:2008**, Information security risk management

– **ISO/IEC 27006:2007**, Requirements for bodies providing audit and certification of information security management systems

– **ISO/IEC 27007**, Guidelines for information security management systems auditing

– **ISO/IEC 27011:2008**, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Segurança da informação

PCI-DSS

- **P**ayment **C**ard **I**ndustry – **D**ata **S**ecurity **S**tandard
- Versão 1.1 em Setembro de 2006;
- Versão 1.2 em Outubro de 2008;
- Versão 1.2.1 em Julho de 2009;
- Desenvolvido para aprimorar a segurança dos dados do portador do Cartão de Pagamento.

Segurança da informação

PCI Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível

Construir e Manter uma Rede Segura

Requisito 1:	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão
Requisito 2:	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança

Proteger os Dados do Portador do Cartão

Requisito 3:	Proteger os dados armazenados do portador do cartão
Requisito 4:	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas

Manter um Programa de Gerenciamento de Vulnerabilidades

Requisito 5:	Usar e atualizar regularmente o software antivírus
Requisito 6:	Desenvolver e manter sistemas e aplicativos seguros

Implementar Medidas de Controle de Acesso Rigorosas

Requisito 7:	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios
Requisito 8:	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador
Requisito 9:	Restringir o acesso físico aos dados do portador do cartão

Monitorar e Testar as Redes Regularmente

Requisito 10:	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão
Requisito 11:	Testar regularmente os sistemas e processos de segurança

Manter uma Política de Segurança de Informações

Requisito 12:	Manter uma política que aborde a segurança das informações

Segurança da informação

Bibliografia:

- Norma ISO/IEC 27001 – Tecnologia da informação - Código de Prática para Gestão da Segurança de Informações.
- Network Security Essentials: Aplications and Standards, Stallings, W., Prentice Hall, 2001.
- Introduction to Computer Security – NIST Handbook 800-12, http://csrc.nist.gov/publications/nistpubs/800-12/ .
- https://www.pcisecuritystandards.org/
- http://abnt.iso.org