Instituições Padronizadoras e Normas de Segurança

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Roteiro

- Histórico
- BS7799
- ISO/IEC 17799:200
  - NBR ISO/IEC 17799
- COBIT

Histórico

- Civilização Egípcia
  - Somente as “castas” superiores podiam ter acesso aos manuscritos
- *Time-sharing*
  - Necessidade de controle dos recursos ou informações
- The Orange Book
  - Resultado de várias pesquisas para segurança
  - Marco zero para a ISO 17999

BS7799

- *Code of Practice for Information Security Management*
- Norma britânica
  - Exigência para negócios com o governo
- Deu origem a ISO 177999
- 2 Partes
  - 1ª Boas práticas
  - 2ª *Framework* para aplicação da segurança

ISSO/IEC 17799:2000 - Parte 1

- Política de Segurança
- Organização da Segurança
- Gestão de Ativos
- Segurança de Pessoal
- Gestão da Segurança Física
- Procedimentos de Operação de Processamento de Dados e de Rede
- Controle de Acesso
- Procedimentos de Desenvolvimento e Manutenção de Sistemas
- Gestão da Continuidade de Negócios
- Aderência à Legislação

COBIT

- *Control Objectives for Information and related Technology*
- Melhores práticas e metodologias
  - Códigos de conduta
  - Critérios de qualificação para os sistemas e processos de TI
  - Padrões profissionais para controle interno e auditoria
- Orientação para os negócios

COBIT
Orientação para os negócios

- Da administração e gerência, visando equilibrar os riscos e os investimentos em controles no ambiente dinâmico de TI.
- Dos usuários, que dependem dos serviços de TI e seus respectivos controles e mecanismos de segurança para realizar suas atividades.
- Dos auditores, que podem utilizá-lo para validar suas opiniões ou para recomendar melhorias dos controles internos à administração.

COBIT

- Processos de TI em 4 domínios diferentes
  - Planejamento e Organização
  - Aquisição e Implementação
  - Entrega e Suporte
  - Monitoramento
- Contém
  - 34 objetivos de Controle de alto nível
    - Suportados pelos guias de auditoria
  - 318 objetivos detalhados para os processos de TI
  - Guias de Gerenciamento

Outras Normas ou Certificações Aplicáveis a Segurança

- Módulo Security
  - (www.modulo.com.br)
- *Project Management Institute*
  - (www.pmi.org)
- *The CISSP and SSCP Open Study Guides*
  - (www.cccure.org)
- *Information Systems Audit and Control Association*
  - (www.isaca.org)
- *SANS Institute - Computer Security Education and Information Security Training*
  - (www.sans.org)

Finalizando

- A aderência as normas demonstra
  - Seriedade da empresa
  - Compromisso com a qualidade
    - Similar a ISO 9000
      - A qualidade não acaba no produto
  - Requisito para atuar em algumas áreas
    - Exigências governamentais ou legais
- Outras normas e metodologias podem ser aplicadas a segurança
  - CMM, SPICE, SEI, etc.

Então....

- Dúvidas ??
- Perguntas ??
- Comentários ??