Aula ao Vivo 1

Escola Politécnica

Segurança de Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

NORMAS ISO

Normas ISO

- 15.408 – Segurança no Desenvolvimento de Software
- 16.167 – Classificação da Informação
- 22.301 – Continuidade de negócios
- 27.000 – Tecnologia da Informação

ISO 15.408
Segurança no Desenvolvimento de Software

ISO 15.408

- Segurança em Desenvolvimento de Software:
  - Ambiente de desenvolvimento
  - Aplicação desenvolvida
  - Garantia de segurança

- **Abrangência:**
  - **Ambiente e estratégias**
  - **Proteção dos dados**
  - **Auditoria**
  - **Autenticação**
  - **Criptografia**
  - **Rejeição & canais seguros**

- **Abrangência:**
  - **Autoproteção**
  - **Gerenciamento de segurança**
  - **Uso dos recursos**
  - **Garantia da segurança**
  - **Testes de segurança**
  - **Análise de Vulnerabilidades**

16.167 – Classificação da Informação

16.167

- Segurança da Informação – Diretrizes para:
  - Classificação
  - Rotulação
  - Tratamento

22.301 – Continuidade de negócios

ISO 22.301

- Sistema de Gestão da Continuidade dos Negócios
  - Requisitos

ISO 22.301

- Gestão da Continuidade dos Negócios
  - O modelo PDCA
  - Escopo do sistema
  - Análise de impacto
  - Avaliação de riscos

27.000 – Tecnologia da Informação

ISO 27.000

- ISO 27.001
  - Sistema de Gestão da Segurança da Informação
  - Controles e objetivos dos controles

ISO 27.000

- ISO 27.002
  - Técnicas de Segurança
  - Código de Prática para controles de segurança da informação

ISO 27.000

- ISO 27.002
  5. Políticas
  6. Organização
  7. Recursos humanos
  8. Ativos
  9. Controle de Acesso
  10. Segurança física e do ambiente

ISO 27.000

- ISO 27.002
  11. Segurança nas operações
  12. Segurança nas comunicações
  13. Aquisição, desenvolvimento e manutenção de sistemas
  14. Supply Chain
  15. Gestão de incidentes
  16. Gestão da Continuidade dos Negócios
  17. Conformidade

ISO 27.000

- ISO 27.003
  - Técnicas de Segurança
  - Diretrizes para a implantação de um sistema de gestão da segurança da informação

ISO 27.000

- ISO 27.004
  - Técnicas de Segurança
  - Gestão da segurança da informação - Métricas

ISO 27.000

- ISO 27.005
  - Técnicas de Segurança
  - Gestão de riscos da segurança da informação

ISO 27.000

- ISO 27.007
  - Diretrizes para auditoria de sistemas de gestão da segurança da informação

ISO 27.000

- ISO 27.037
  - Tecnologia da Informação
  - Técnicas de Segurança
  - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital

Referências

- ABNT. Coletânea de Normas Técnicas – Segurança da Informação. Rio de Janeiro: ABNT, 2014
- ALBUQUERQUE, R. Segurança no desenvolvimento de software: como garantir a segurança do sistema para seu cliente usando a ISO/IEC 15.408. Rio de Janeiro: Campus, 2002.