PLANO DE ENSINO

Disciplina: Segurança em Sistemas de Informação
Carga Horária: 60h
Período: 6º

Ementa

Política de Segurança de Informações. Controles de Acesso Lógico. Controles de Acesso Físico. Controles Ambientais. Plano de Contingências e Continuidade dos Serviços de Informática. Conformidade com a Norma ISO 17799. Estudos de Caso.

Objetivos

Conhecer as principais formas de ataque e manipulação de informações de forma não autorizada em sistemas telemáticos bem como as medidas de segurança a serem tomadas com o intuito de garantir a segurança da informação sob a luz da norma de Segurança da Informação.

Conteúdo Programático

Unidade I: Política de Segurança de Informações

1.1. Objetivos de Segurança

1.2. Comprometimento da Gerência Superior

1.3. Legislação Brasileira e Instituições Padronizadas

1.4. Definição de uma Política de Segurança de Informações

1.5. Identificação dos Recursos

1.6. Análise de Riscos

1.7. Análise de Ameaças

1.8. Análise de Impactos e Cálculo de Riscos

1.9. Controles de Segurança

1.10. Definição de Serviços de Segurança

1.11. Definição de Mecanismos de Segurança

1.12. Ataques

1.13. Implantação de Gerência de Segurança

1.14. Implementação e Auditoria de Políticas de Segurança

Unidade II: Controles de Acesso Lógico

2.1. Recursos e Informações a serem Protegidos

2.2. Elementos Básicos de Controle de Acesso Lógico

2.3. Processo de Logon

2.4. Proteção aos Recursos

2.5. Direitos e Permissões de Acesso

2.6. Monitoramento

2.7. Controles de Acesso Lógico

2.8. Gerência de Controle de Acesso Lógico

2.9. Riscos Inerentes a Controles de Acesso Lógico Inadequados

2.10. Lista de Verificações

Unidade III: Controle de Acesso Físico

3.1. Recursos a serem Protegidos

3.2. Controles Administrativos

3.3. Controles Explícitos

3.4. Definição dos Controles Físicos

3.5. Riscos Inerentes a Controles Físicos Inadequados

3.6. Lista de Verificações

Unidade IV: Controles Ambientais

4.1. Incêndios

4.2. Energia Elétrica e Descargas Elétricas Naturais

4.3. Enchentes ou outras Ameaças que envolvam Água

4.4. Temperatura, Umidade e Ventilação

4.5. Limpeza e Conservação

4.6. Riscos Inerentes a Controles Ambientais Inadequados

4.7. Lista de Verificações

Unidade V: Plano de Contingências e Continuidade dos Serviços de Informática

5.1. Necessidade do Plano de Contingências

5.2. Fases do Planejamento de Contingências

5.3. Atividades Preliminares

5.4. Análise do Impacto

5.5. Análise das Diversas Alternativas de Recuperação

5.6. Desenvolvimento do Plano de Contingências

5.7. Treinamento

5.8. Teste

5.9. Atualização do Plano

5.10. Lista de Verificações

Unidade VI: Conformidade com a Norma ISO 17799

6.1. Framework e os Controles de Segurança

6.2. Teste de Conformidade

Unidade VII: Estudos de Casos

7.1. Análise de Políticas de Segurança Implementadas

7.2. Levantamento crítico de falhas

7.3. Sugestões de mudanças

7.4. Construção de Políticas de Segurança com Simulação

Unidade VIII: ITIL

8.1.Importância, Normas e aplicações

8.2.Gerenciamento:

8.2.1.Nível de Serviços – Disponibilidade - Segurança da Informação – Fornecedores - Capacidade - Continuidade dos Serviços de TI – Eventos – Incidentes - Problemas

8.3.Processo de melhoria continua Ciclo de Deming

Unidade IX: MODELO COBIT

9.1. A evolução da Função TI ao longo dos anos

9.2. A importância de TI e como as questões de TI afetam as organizações

9.3. Como o COBIT® pode ajudar na Governança de TI

9.4. Estrutura do COBIT® - Objetivos de Controle, Práticas de Controle,

Diretrizes de Gerenciamento, Diretrizes de Auditoria

9.5 Os benefícios e desvantagens do uso de controles

Unidade X: Norma Internacional de Segurança ISO/27002

Bibliografia Básica

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. ABNT, 2005.

DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação*. 1. ed. Rio de Janeiro: Axcel Books, 2000.

SÊMOLA, Marcos. *Gestão da segurança da informação*: uma visão executiva. 1. ed. Rio de Janeiro: Elsevier, 2003.

BON, JAN VAN - *Editor, Fundamentos do Gerenciamento de Serviços de TI baseado na ITIL*, Van Haren Publishing, 2006.

ISACA, COBIT 5 for Information Security, ISACA, 2012.

Bibliografia Complementar

S. Burnett, S. Paine , *Criptografia e Segurança* – O Guia Oficial RSA, 2002.

TANENBAUM, Andrew S. Redes de computadores. 5. ed. Rio de Janeiro: Campus, 2003.

SOARES, Luiz Fernando G.; LEMOS, Guido; COLCHER, Sergio. *Redes de computadores*: das LANs, MANs e WANs as redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

C. KAUFMAN, R. Perlman, M. Speciner Network Security – *Private Communication in a Plublic World* – 2nd ed., Prentice Hall, 2002.

SCHNEIER, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, 1996.

SCHNEIER, Bruce. Secrets and Lies: Digital Security in a Networked World, 2nd ed., John Wiley & Sons, 2000.