SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 01: PLANO DE ENSINO INTRODUÇÃO AO TEMA

SUMÁRIO

Fatec Mauá

1. Objetivo da Aula – Tópico da Ementa

2. Prof. Marco Antônio TOMÉ

3. Plano de Ensino da Disciplina: ISG-022
   Segurança no Desenvolvimento
   de Aplicações (SDA)

4. Alunos – Grupos de Trabalho

5. Introdução: Segurança da Informação (SI)

1. OBJETIVO E EMENTA

Fatec Mauá

- **Objetivo da Aula**

  Aula inaugural, apresentações do professor e dos alunos, divulgação do plano de ensino, planejamento da disciplina, descrição do plano de aulas e introdução ao tema da disciplina: Segurança da Informação (SI).

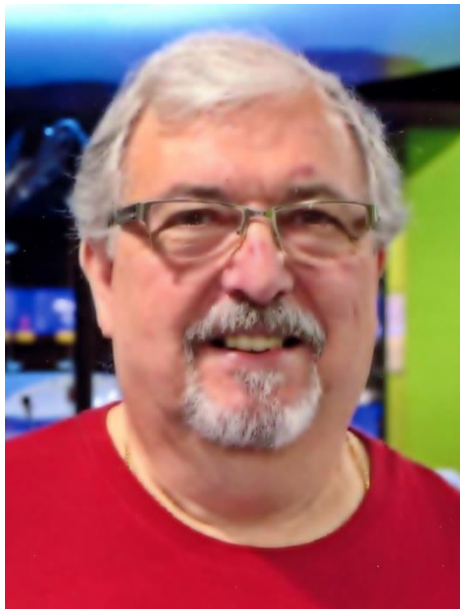
- **Tópico da Ementa**

  Conceitos fundamentais do pilar de segurança.

2. PROF. MARCO ANTÔNIO TOMÉ

Fatec Mauá

➢ Pessoal e formação:



- Brasileiro, 69 anos, casado, dois filhos e duas netas.
- Professor da Fatec e Consultor.
- Mestre em Administração: Governança Corporativa pela FMU-Faculdades Metropolitanas Unidas
- Pós-graduado/Especialista (lato sensu) em Auditoria e Controladoria pela Faculdade São Judas
- Graduado no curso de Tecnologia em Processamento de Dados pela UNESP/FATEC.

2. PROF. MARCO ANTÔNIO TOMÉ

Fatec Mauá

➢ Experiência Profissional:

- Consultor e Professor de Governança e Auditoria de TI
- Experiência profissional (mais de 38 anos), atuando como empregado e/ou consultorias em Governança e Gestão de TI, Auditoria de Sistemas, Segurança e Sistemas da Informação
- Coordenador de cursos de graduação: Bacharelado e Tecnologia da área de computação – Coordenador acadêmico de unidades de ensino superior (cerca de 10 anos)
- Professor de disciplinas de tecnologia da informação em cursos técnicos do ensino médio, de graduação do ensino superior e de pós-graduação/especialização (mais de 30 anos)
- Professor em Bancas de Concursos Públicos para elaboração, aplicação e correção de provas objetivas e práticas de TI

3. PLANO DE ENSINO

Fatec Mauá

- Curso Superior de Tecnologia (CST) em **Desenvolvimento de Software Multiplataforma (DSM)**

- Disciplina – **ISG-022 – Segurança no Desenvolvimento de Aplicações (DAS)**

- Carga Horária
  Semanal: **04 horas-aulas**
  Semestral: **80 horas-aulas**

3. PLANO DE ENSINO

Fatec Mauá

➢ Ementa da Disciplina . . .

- Conceitos fundamentais do pilar de segurança: confidencialidade, integridade, disponibilidade e autenticidade.
- Gestão de Vulnerabilidades e resposta à incidentes de segurança.
- Redução da superfície de ataque, defesa em profundidade, menor privilégio, padrões seguros, modelagem de ameaças.

3. PLANO DE ENSINO

Fatec Mauá

➢ Ementa da Disciplina

- ferramenta para diagramação e enumeração de ameaças, testes de segurança,
- Fuzz testing, Teste de invasão, Injeção de SQL, Cross-Site Scripting (XSS),
- aplicação de conceitos de OWASP (Open Web Application Security Project) e
- SDL (Security Development Lifecycle),
- Revisão de código.

3. PLANO DE ENSINO

Fatec Mauá

➢ Objetivo da Disciplina ...

- Compreender o pilar de Segurança da Informação (SI) e empregar técnicas de programação segura para o desenvolvimento de aplicações Web, na proteção dos dados de entrada dos usuários.
- Conhecer e utilizar conceitos de SQL Injection, para testar as vulnerabilidades das aplicações.

3. PLANO DE ENSINO

Fatec Mauá

➢ Objetivo da Disciplina

- Aplicar técnicas de validação ou codificação, para assegurar as mensagens enviadas ao navegar.
- Realizar armazenamento seguro das informações, com a utilização de autenticidade e criptografia.

3. PLANO DE ENSINO

Fatec Mauá

➢ Metodologia Proposta

- Aulas expositivas teórica e prática.
- Aprendizagem baseada em projetos/problemas.
- Gamificação.
- Sala de aula invertida.
- Estudo de caso real.
- Utilização de simuladores e ambientes virtuais.
- Trabalhos interdisciplinares, segundo o Manual de Projetos Interdisciplinares

3. PLANO DE ENSINO

Fatec Mauá

➢ Critério de Avaliação

- **MédiaF** = ((P1*0,35)+(P2*0,35)+(T*0,3))
  onde,
  P1 = nota da prova P1 (de 0 a 10)
  P2 = nota da prova P2 (de 0 a 10)
  P3 = nota da prova substitutiva (de 0 a 10)
  T = média de trabalho e atividades (de 0 a 10)

- **Aprovação**
  MédiaF ≥ 6,0 e
  Frequência ≥ 75%

3. PLANO DE ENSINO

Fatec Mauá

- **Plano de Aulas . . .**

1. T01 - Apresentações, Planejamento e Introdução à Segurança da Informação (SI)
2. T02 - Conformidade e os Aspectos Legais da SI
3. T03 - Controles de Acesso e Autorização
4. T04 - Autenticação e Gestão de Sessões
5. T05 - Testes de Segurança em Aplicações

3. PLANO DE ENSINO

Fatec Mauá

- **Plano de Aulas . . .**

6. T06 - Prevenção de XSS e SQL Injection
7. T07 - Logs e Monitoração de Aplicações
8. P1 - Semana de Avaliação Oficial
9. P1 - Divulgação da Nota P1 e Revisão de Conteúdo
10. T08 - Validação e Sanitização de Dados

3. PLANO DE ENSINO

Fatec Mauá

- **Plano de Aulas . . .**

11. T09 - Fundamentos de Criptografia
12. T10 - Criptografia em Aplicações e Dados
13. T11 - Introdução à Programação Segura
14. T12 - Segurança em Aplicações Web
15. T13 - Desenvolvimento de Aplicações Web Seguras

3. PLANO DE ENSINO

Fatec Mauá

- **Plano de Aulas**

16. T14 - Revisão do Principais Tópicos do Curso
17. P2 - Semana de Avaliação Oficial
18. P2 - Divulgação da Nota P2 e Revisão de Conteúdo
19. P3 - Recuperação e Avaliação de Atividades
20. Fechamento do Semestre Letivo

3. PLANO DE ENSINO

Fatec Mauá

- **Bibliografia Básica**

1. MORENO D. **Pentest em aplicações web.** São Paulo: Novatec, 2017.

2. MUELLER J. P. **Segurança para desenvolvedores web.** São Paulo: Novatec, 2016.

3. SEITZ J. **Black Hat Python: Programação Python Para Hackers e Pentesters.** São Paulo: Novatec, 2015.

3. PLANO DE ENSINO

Fatec Mauá

- **Bibliografia Complementar**

1. ABNT. **Tecnologia da informação - Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799).** Rio de Janeiro, RJ: 2001.
2. FERREIRA, Rodrigo. **Segurança em aplicações Web.** São Paulo: Casa do Código, 2017.
3. WEIDMAN G. **Testes de Invasão: Uma introdução prática ao hacking.** São Paulo: Novatec, 2014.

4. ALUNOS – GRUPOS DE TRABALHO

Fatec Mauá

➢ **Apresentação dos Alunos da Turma**

- Identificação e breve apresentação dos alunos presentes na sala de aula.

➢ **Formação de Grupos de Trabalho**

- Identificação dos grupos de trabalho.
- Relação de participantes de cada grupo.
- Indicar o representante de cada grupo.

➢ **Atividade em Grupo**

- Descrição . . .

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

➢ **Tópicos** do Capítulo:

- Definições de **conceitos**
- Definição de **segurança da informação**
- Modelos de segurança da informação

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

➢ Definições de **"Conceitos"**

- **Informação:** um **ativo essencial** às **pessoas** e aos negócios das **organizações**, de quaisquer tipos e tamanhos, que é **coletado, processado, armazenado** e **transmitido**, permitindo que **decisões** e **ações** sejam tomadas.

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

➢ Definições de **"Conceitos"**

- **Ativo:** qualquer coisa que tenha **valor** para as **pessoas** ou para as **organizações**.

- **Ameaça:** ocorrência de um **ataque**, por algo ou alguém, que tem um **potencial** de causar **perda**, **dano** ou **prejuízo** a qualquer **ativo**, inclusive a **informação**.

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

- Definições de **"Conceitos"**

- **Risco:** a **probabilidade** de uma **ameaça** ter sucesso, ou seja, a **possibilidade** de ocorrer um **evento** que poderá levar a **resultados negativos**, afetando um **ativo** e provocando **impactos** às pessoas ou às organizações com **perdas**, **danos** ou **prejuízos**.

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

- Definições de **"Conceitos"**

- **Gestão de Risco:** uma **prática essencial** para tratar as **incertezas** de diversos tipos de riscos, **identificando**, **avaliando** e **priorizando** os riscos, aplicando recursos para **minimizar**, **monitorar** e **controlar** as **probabilidades** ou os **impactos** desses eventos adversos.

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

- Definição:
  "Segurança da Informação (SI)"

- Uma prática de Gestão de Risco que envolve a implementação de **controles apropriados**, ou seja, **medidas de segurança** e **de proteção de dados,** contra uma gama de **ameaças**, com objetivo de **eliminar** ou **mitigar** os **riscos** e as suas **consequências**, garantindo a **integridade**, a **disponibilidade** e a **confidencialidade** das **informações**.

5. SEGURANÇA DA INFORMAÇÃO (SI)

Fatec Mauá

➢ Definições de **"Conceitos"**

- **Informação:** ativo essencial ao negócio de uma organização, de qualquer tipo ou tamanho, que é coletado, processado, armazenado e transmitido.

- **Ameaça:** ocorrência de ataque, erro, desastre ou inerente ao uso, que qualquer ativo está sujeito, inclusive a informação

SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 01: PLANO DE ENSINO INTRODUÇÃO AO TEMA