FACULDADE SUMARÉ
PLANO DE ENSINO

Curso: Sistemas de Informação	**Semestre Letivo / Turno**:
Disciplina: Segurança em Desenvolvimento de Sistemas	**Professor**:
Carga Horária: 50h/a	**Período**:

Dados de acordo com o Projeto do Curso:

Ementa da disciplina:	Usando metodologias de mercado, normas internacionais e ferramentas disponíveis na Internet, os alunos serão capacitados nas técnicas de desenvolvimento seguro, análise de riscos e implementação do SDL, possibilitando que o aprendizado seja utilizado para incluir os aspectos necessários de segurança nos processos de desenvolvimento e/ou manutenção de software.
Objetivos Gerais:	O curso "Desenvolvimento Seguro - Security Development Lifecycle (SDL) "e Desenvolvimento Seguro de Aplicações Web é ideal para profissionais que buscam entender as questões de segurança em aplicações, estudando instrumentos de análise proativa e como estes devem ser utilizados. O curso segue e ensina as melhores práticas no desenvolvimento seguro, além de incorporar a segurança das informações em todo o ciclo de vida do desenvolvimento dos softwares.
Conteúdo:	1. Introdução ao Desenvolvimento Seguro 2. Por que segurança em desenvolvimento 3. O processo de segurança em desenvolvimento 4. Papéis e Responsabilidades
Bibliografia Básica:	TERADA,Routo. SEGURANÇA DE DADOS: CRIPTOGRAFIA EM REDES DE COMPUTADORES. 2. ed. São Paulo: Editora Edgard Blücher Ltda., 2008. CARUSO, Carlos A.A.; STEFFEN, Flávio Deny. SEGURANÇA EM INFORMÁTICA E DE INFORMAÇÕES. 3. ed. São Paulo: Senac, 2006. LAUDON, Kenneth C.; LAUDON, Jane Price . SISTEMAS DE INFORMAÇÃO GERENCIAIS. Tradução Thelma Guimarães. 7ª. ed. São Paulo: Prentice Hall, 2007.
Bibliografia Complementar:	O'BRIEN, James A.. SISTEMAS DE INFORMAÇÃO E AS DECISÕES GERENCIAIS NA ERA DA INTERNET. Tradução Cid Knipel Moreira. São Paulo: Saraiva, 2002. MARCACINI, A. T. R. DIREITO E INFORMÁTICA: UMA ABORDAGEM JURÍDICA SOBRE CRIPTOGRAFIA. Rio de Janeiro: Forense, 2005 ASSUNÇÃO, Marcos Flavio Araujo. SEGREDOS DO HACKER ETICO. São Paulo: Visual Books, 2012
Critérios de Avaliação:	**1º Bimestre** – Avaliação Escrita Individual (60%) + Trabalho de Pesquisa e seminário (20%) + Avaliação Institucional (20%) **2º Bimestre** – Avaliação Escrita Individual (60%) + Trabalho de Pesquisa em grupo (40%) **Média Final =** (Nota 1+Nota 2)/2

Data:	**Assinatura do Professor:**	**Assinatura do Coordenador:**

Programação Aula a Aula

Aulas	Objetivos / Conteúdo
Semana 01	Aula Inicial
Semana 02	Introdução ao Desenvolvimento Seguro
Semana 03	Por que segurança em desenvolvimento
Semana 04	O processo de segurança em desenvolvimento
Semana 05	Papéis e Responsabilidades
Semana 06	Introdução a Modelagem de Ameaças
Semana 07	As Vulnerabilidades do OWASP Top
Semana 08	Injeção
Semana 09	Cross-Site Scripting (XSS) e CSRF
Semana 10	Avaliação P1.
Semana 11	Segurança por Código
Semana 12	Práticas Gerais de Código Seguro
Semana 13	Autenticação e Gerenciamento de Senhas
Semana 14	Gerenciamento de Sessão
Semana 15	Suporte na Revisão e Desenvolvimento
Semana 16	Métricas de Acompanhamento
Semana 17	Gestão de Vulnerabilidades e Resposta à Incidentes de Segurança
Semana 18	Avaliação P2.
Semana 19	Prova Substitutiva.
Semana 20	Exame.