FACULDADE SUMARÉ
PLANO DE ENSINO

Curso:	**Semestre Letivo / Turno**:
Disciplina: Segurança da Informação	**Professor**:
Carga Horária:	**Período**:

Dados de acordo com o Projeto do Curso:

Ementa da disciplina:	A disciplina aborda os princípios em segurança da informação. Análise de riscos. Leis, normas e padrões de segurança da informação. Auditoria de sistemas. Autenticação e controle de acesso. Aspectos tecnológicos da segurança da informação. Plano de continuidade do negócio. Boas práticas em segurança da informação.
Objetivos Gerais:	Entender necessidades de segurança em ambiente de Redes. Conhecer e aplicar técnicas de planejamento de segurança em ambiente de rede. Conhecer e aplicar técnicas de implementação e avaliação de políticas de segurança. Compreender as tecnologias disponíveis para garantia da segurança contra vírus, restrição de acesso e manutenção. Distinguir as técnicas e ferramentas de segurança da informação. Compreender os conceitos aplicáveis à criptografia de informações e a identificação, autenticação e autorização de acesso. Compreender as normas padrão de segurança: ISO/IEC 27002/2005; ISO/IEC 17799/2000; BS 7799; NBR/ISO 17799; e publicações sobre segurança do NIST – National Institute of standards and Tecnology e IETF (RFC´s). Conhecer as práticas pedagógicas para conscientização dos usuários de computadores sobre a importância de obediência às políticas de segurança da empresa. Entender e aplicar a arquitetura de gerenciamento da Política de Segurança com propósito de monitorar e melhorar a performance do sistema, incluindo informes de incidentes, nível de aderência, auditoria interna e revisões.
Conteúdo:	1. Introdução a Segurança da Informação 2. Conhecer e aplicar técnicas de Segurança da Informação em Ambientes de Rede 3. Desenvolver e aplicar políticas de Segurança da Informação 4. Conhecer e aplicar as principais técnicas de Segurança da Informação 5. Normas de padrão segurança 6. Auditoria de segurança 7. Práticas pedagógicas de conscientização de usuários
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	Introdução à Segurança da Informação; Princípio e conceitos fundamentais de Segurança da Informação.
Semana 02	Distinguir técnicas e ferramentas de segurança da informação; Tecnologias segurança contra vírus e outros ameaças.
Semana 03	Gerenciamento de acessos; Validação de dados de entrada e de saída; Criptografia e PKI.
Semana 04	Normas padrão de segurança: ISO/IEC 17799/2000; BS 7799; NBR/ISO 17799.
Semana 05	Normas padrão de segurança: ISO/IEC 27002/2005.
Semana 06	Publicações sobre segurança do NIST – National Institute of standards and Tecnology e IETF (RFC´s).
Semana 07	Compreender os conceitos aplicáveis à criptografia de informações e a identificação, autenticação e autorização de acesso.
Semana 08	Introdução ao Sistema de Gestão da Segurança da Informação (SGSI).
Semana 09	Tipos de ameaça humanas e não humanas, intencional e não intencional.
Semana 10	Avaliação P1.
Semana 11	Interrupções básicas e interrupção no ambiente físico.
Semana 12	Danos diretos e indiretos; Expectativas de Perdas (Perda anual e Perda única).
Semana 13	Ciclo de incidentes; Tipos de medidas de ciclos de incidentes.
Semana 14	Medidas físicas; Cabeamento, equipamento e anéis de proteção.
Semana 15	Planejando e Iniciando uma auditoria ISO/IEC27001:2013; Os procedimentos de auditoria: observação, análise de documentos, entrevistas, técnicas de amostragem, verificação técnica, comprovação e avaliação.
Semana 16	Desenvolver e aplicar políticas de Segurança da Informação.
Semana 17	Práticas pedagógicas de conscientização de usuários.
Semana 18	Avaliação P2.
Semana 19	Prova Substitutiva.
Semana 20	Exame.