Campus: São José dos Campos		
Curso (s): BCC/EC/BCT		
Unidade Curricular (UC): SEGURANÇA COMPUTACIONAL		
Unidade Curricular (UC): *[nome da UC em inglês] COMPUTER SECURITY*		
Unidade Curricular (UC): *[nome da UC em espanhol - opcional]*		
Código da UC:		
Docente Responsável/Departamento: Valério Rosset		Contato (e-mail): *[opcional]* vrosset@unifesp.br
Docente (s) Colaborador/a (es/as)/Departamento (s):		Contato (e-mail): [opcional]
Ano letivo: 2022	Termo:	Turno/Turma: I/N
Nome do Grupo/Módulo/Eixo da UC (se houver):		Idioma predominante em que a UC será oferecida: (x) Português ( ) English ( ) Español ( ) Français ( ) Libras ( ) Outro:
UC: ( ) Fixa (x) Eletiva ( ) Optativa	Oferecida como: (x) Disciplina ( ) Módulo ( ) Estágio ( ) Outro:	Oferta da UC: (x) Semestral ( ) Anual
Ambiente Virtual de Aprendizagem: (x) Moodle (x) Classroom ( ) Outro: ( ) Não se aplica		
Pré-Requisito (s) - Indicar Código e Nome (s) da (s) UC: Sistemas Operacionais		
Carga horária total (em horas): 72		
Carga horária teórica (em horas): 36	Carga horária prática (em horas): 36	Carga horária de extensão (em horas, se houver):
Se houver atividades de extensão, indicar código e nome do projeto ou programa vinculado na Pró-Reitoria de Extensão e Cultura (ProEC):		
Ementa: *Introdução a segurança computacional; ataques e ameaças de segurança; políticas de segurança; mecanismos de segurança, criptografia, autorização e controle de acesso, autenticação; segurança em sistemas operacionais e software; aplicações de segurança em redes e Internet; técnicas e ferramentas para testes de penetração;*		
Conteúdo programático: *Introdução a Segurança Computacional. Ameaças de Segurança Ataques e Vulnerabilidades. Ferramentas para Teste de Penetração. Políticas de Segurança. Criptografia. Criptografia Simétrica. Cifra de Bloco. DES. AES. criptografia de chave Pública. RSA. Funções Hash. Autenticação. Protocolos e Mecanismos de Autenticação. Autorização e Controle de Acesso. Modelos de Controle de Acesso. Mecanismos de controle de Acesso. Segurança em Sistemas Operacionais. Segurança no Windows. Segurança no Linux/Unix. Aplicações de segurança em Redes e Internet. Aplicações de Autenticação. IPSec. Segurança na Web. Firewalls.*		
Objetivos: <u>Gerais:</u> Apresentar os principais conceitos e técnicas relacionadas à segurança computacional e suas aplicações em redes de computadores e internet. <u>Específicos:</u>		

Ao final do curso o aluno deverá estar familiarizado com as principais ameaças de seguranças e técnicas de prevenção de fraudes, incluindo algoritmos de criptografia simétrica, algoritmos de criptografia assimétrica, modelos de controle de acesso e ferramentas de avaliação de segurança.

Metodologia de ensino:
O curso será baseado em aulas expositivas com auxílio do quadro e projetor multimídia. A participação dos alunos em sala de aula será estimulada através de perguntas e sessões de exercícios. Para fixação dos tópicos estudados, os alunos receberão, ao longo do curso, listas de exercícios para entrega em sala de aula. Por fim, destacamos as aulas práticas nos laboratórios de informática para implementação de protótipos.

Avaliação:

A avaliação será feita através de uma prova teórica (P1), um seminário (SE), e trabalhos práticos. A média dos trabalhos práticos (TP) irá compor a nota final, que será uma média ponderada das avaliações supracitadas, como definido a seguir:

Nota final = 0,3 x P1 + 0,3 x SE + 0,4 x TP

* Poderá haver ainda de um trabalho prático especial (TPE) de maior escala que poderá substituir a nota do SE.

Bibliografia:
[deve ser indicada a bibliografia necessária para a UC]

Básica:

1. STALLINGS, William. Criptografia e seguranças de redes: princípios e práticas. 4 ed. Säo Paulo: Person Prentice-Hall, 2008. 492 p p. ISBN 978-85-7605-119-0. Título original: Criptography and networking security 4/E.
2. Cole, Eric; Krutz, Ronald; Conley, James W.. Network security bible. 2nd ed. Indianapolis: Wiley, 2009. 891 p. ISBN 978-0-470-50249-5.
3. Charles P. Pfleeger, Shari Lawrence Pfleeger. Security in Computing, 4th ed. Prentice Hall, 2007.

Complementar:

1. Kaufman, Charlie. Network security: private communication in a public world. 2.ed. Upper Saddle River (EUA): Prentice-Hall, c2002. 713 p. ISBN 9780130460196.
2. Panko, Raymond R.. Corporate computer and network security. 2. ed. Upper Saddle River, NJ: Prentice Hall, 2010. 502 p. ISBN 978-0-13-185475-8.
3. Stallings, William. Cryptography and network security: principles and practice. 5.ed. Upper Saddle River, NJ: Prentice Hall, 2011. 719 p.
4. KUROSE, James F.; Ross, Keith W.. Redes de computadores e a internet: uma abordagem topdown. 5.ed. São Paulo: Addison-Wesley, 2010. 614 p. ISBN 9788588639973.
5. Tanenbaum, Andrew S; Wetherall, David. Redes de computadores. [Computer networks 5th edition]. Tradução Daniel Vieira, Revisão técnica: Prof.Dr. Isaias Lima. 5 ed. Rio de Janeiro: Elsevier, 2011. 582 p. ISBN 978-85-7605-924-0.

Cronograma: *[opcional]*