UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Computação
Av. João Naves de Ávila, nº 2121, Bloco 1A - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4144 - http://www.portal.facom.ufu.br/ facom@ufu.br

PLANO DE ENSINO

1. IDENTIFICAÇÃO

Componente Curricular:	Segurança da Informação							
Unidade Ofertante:	Faculdade de Computação							
Código:	GBC083		Período/Série:		8º		Turma:	C
Carga Horária:						Natureza:		
Teórica:	60	Prática:	00	Total:	60	Obrigatória:	X	Optativa: ( )
Professor(A):	Ivan da Silva Sendin					Ano/Semestre:		2021/02
Observações:								

2. EMENTA

Breve histórico da criptografia clássica e moderna. Conceituação de sistemas simétricos e assimétricos. Principais algoritmos simétricos e assimétricos de ciframento. Principais algoritmos para ”hashing” criptográfico. Principais algoritmos para assinaturas digitais. Protocolos para negociação de chaves. Protocolos para autenticação em sistemas distribuídos. Protocolos IPSec, SSL e TLS. Introdução à Segurança da informação, planejamento de Contingência e Continuidade de Negócios, Políticas e Normas em Segurança. Certificação de sistemas e de software. Segurança em Aplicações, Segurança de Operações, Segurança de Redes e Telecomunicações.

3. JUSTIFICATIVA

Segurança da informação é a atividade que consiste em assegurar a proteção de informação em termos de confidencialidade, integridade e disponibilidade. Atualmente, o uso de sistemas e conceitos de segurança da informação é amplamente difundido para uma grande gama de aplicações, variando desde a segurança em computadores pessoais até em grandes infraestruturas como a Internet.

4. OBJETIVO

Objetivo Geral:
Ao final do custo o aluno conhecerá os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de criptografia. Deverá conhecer e entender os fundamentos de criptografia e funcionamento de algoritmos simétricos e assimétricos. Irá adquirir capacidade de escolher técnicas de criptografia conforme a necessidade. Adicionalmente, o aluno conhecerá e implementará serviços de segurança utilizando diversas APIs criptográficas como o JCA (Java Cryptograhic Architecture) e o OpenSSL.

5. PROGRAMA

O programa da disciplina for organizado da seguinte maneira:

Modulo	Conteúdo
1	Apresentação da Disciplinas. Avaliação. Bibliografia. Oportunidades de atuação em Segurança da Informação. Lendas da segurança da informação. Informação: o que proteger. Risco e Impacto
2	Segredos, senhas e chaves: entropia, Força Bruta e política de senhas. Diceware
3	Criptografia: Cifradores Simetricos.hashing. Cifradores Assimetricos. Assinaturas e TLS/SSL
4	Segurança de Sistemas: política de senhas. Desenvolvimento: buffers e execução de dados. Defesas.Contingencia e continuidade.
5	Segurança de redes TCP/IP e ferramentas

6. **METODOLOGIA**

Cronograma de Atividades Presenciais

Aula	Semana	Data	Modulo	CH	Formato
1	1	3/Maio	1	2	Expositiva
2	1	4/Maio	1	2	Expositiva
3	2	10/Maio	1	2	Expositiva
4	2	11/Maio	1	2	Expositiva
5	3	17/Maio	1	2	Expositiva
6	3	18/Maio	1	2	Expositiva
7	4	24/Maio	2	2	Expositiva
8	4	25/Maio	2	2	Expositiva
9	5	31/Maio	2	2	Expositiva
10	5	1/Junho	Avaliação P1	2	Avaliação
11	6	6/Junho	3	2	Expositiva
12	6	7/Junho	3	2	Expositiva
13	7	13/Junho	3	2	Expositiva
14	7	14/Junho	3	2	Expositiva
15	8	20/Junho	3	2	Expositiva
16	8	21/Junho	3	2	Expositiva
17	9	27/Junho	3	2	Expositiva
18	9	28/Junho	3	2	Expositiva
19	10	5/julho	3	2	Expositiva

Aula	Semana	Data	Modulo	CH	Formato
20	10	6/julho	3	2	Expositiva
21	11	12/julho	Avaliação P2	2	Avaliação
22	11	13/julho	4	2	Expositiva
23	12	19/julho	4	2	Expositiva
24	12	20/julho	4	2	Expositiva
25	13	26/julho	4	2	Expositiva
26	13	27/julho	5	2	Expositiva
27	14	2/agosto	5	2	Expositiva
28	14	3/agosto	5	2	Expositiva
29	15	9/agosto	5	2	Expositiva
30	15	10/Agosto	Avaliação P3	2	Avaliação
31	16	16/Agosto	recuperação de aprendizagem: Exercicios	2	Expositiva
32	16	17/Agosto	recuperação de aprendizagem: Prova	2	Avaliação

Serão ofertadas 4 atividades assincronas de 2 HA cada, essas atividades serão compostas por leituras de artigos, videos, implementações e análises. Cada uma destas atividades será uma avaliação. O conteúdo das atividades tão como as datas de entrega serão definidos durante a execução do curso, quando mais informações (eg. tamanho da turma) estiverem dispiníveis.

A carga horaria composta pelas atividades sincronas é de 64 HA e a carga horaria de atividades assincronas é de 8 HA, totalizando 72 HA.

Os horarios das atividades sincronas ocorrerão conforme o previsto na ficha da disciplina.

O atendimento aos alunos ocorrerá por meio do chat ou de reuniões virtuais previamente agendadas com o professor utilizando a plataforma MS Teams.

7. AVALIAÇÃO

A avaliação será composta por:

- 4 trabalhos referentes as atividades assincronas, cada um com valor de 5 pontos, totalizando 20 pontos;
- P1 e P2 com 20 pontos cada;
- P3 com 40 pontos.

A Nota Final (NF) é dada pela soma dos pontos de cada atividade.

Será oferecia uma prova de Recuperação de aprendizagem com valor de 100 pontos, a nota final pos recuperação é a media aritimética entre a NF e o valor da prova de recuperação.

8. BIBLIOGRAFIA

Básica

- Stallings, William. Criptografia e segurança de redes: princípios e práticas. Prentice Hall, 2008.

- Stallings, William. Network security essential: applications and standards. 2a edição. Prentice Hall, 2003.
- Handbook of applied Cryptography. Alfred J. Menezes, Paul C. Oorschot e Scot A. Vanstone. CRC Press, 1996

Complementar

- Brands, Stefan A. Rethinking public key infrastructures and digital certificates: building in privacy. Cambridge, Mass.: MIT Press, 2000.
- Burnett, Steve. RSA Security's official guide to cryptography. New York: Osborne/McGraw-Hill, 2001.
- Ford, Warwick. Secure electronic commerce: building the infrastructure for digital signatures and encryption. 2a edição. Upper Saddle River, New Jersey. Prentice Hall PTR, 2001.
- Mao, Wenbo. Modern cryptography: theory and practice. Pearson Education India, 2003.
- Stinson, Douglas R. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

DIREITOS AUTORAIS

9. **APROVAÇÃO**

Aprovado em reunião do Colegiado realizada em: ____/____/_____

Coordenação do Curso de Graduação: _____