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:	Tópicos Especiais em Segurança da Informação							
Unidade Ofertante:	Facom							
Código:	GSI078	Período/Série:				Turma:	S	
Carga Horária:						Natureza:		
Teórica:	60	Prática:		Total:	60	Obrigatória: ( )	Optativa:	(X)
Professor(A):	Ivan da Silva Sendin					Ano/Semestre:	2025/2	
Observações:								

2. EMENTA

Segurança e Criptografia: Conceitos Básicos, aplicações e usos. Algoritmos Simétricos. Algoritmos Assimétricos. Hash e Certificados.

3. JUSTIFICATIVA

Blockchain, criptomoedas e contratos inteligentes vem ganhando relevância dentro do contexto do desenvolvimento profissional na área de computação.

4. OBJETIVO

Objetivo Geral:
Capacitar o aluno a compreender e desenvolver aplicações de Blockchain.
Objetivos Específicos:
Consenso Distribuido, protocolos criptográficos, programação de contratos inteligentes.

5. PROGRAMA

Proposta de programa:

- Consenso Distribuído:
  - Encadeamento
  - Prova de Trabalho
- Bitcoin/Criptomoedas
  - Visão Geral
  - Transações
  - pseudo-anonimato
  - analise de Blockchain
- Contratos Inteligentes
  - Programação
  - Deploy

    - Questoes de Segurança
    -
- Aplicações de Protocolos Criptográficos
    - Autenticação
    - Provas de Conhecimento Zero
    - Computação Segura Multiparte

6. METODOLOGIA

O curso será ministrado através de aulas expositivas sobre o tema, aos sábados conforme estabelecido pela Coordenação. Para a exposição, serão usados slides, disponibilizados em meio virtual, em conjunto com a exposição oral do professor. A apresentação será complementada, sempre que necessário, com anotações e demonstrações no quadro da sala. Serão ao todo 62 horas-aula presenciais. As 10 horas faltantes serão contabilizadas por meio da realização de Atividades extraclasse distribuídas ao longo do semestre.

1. 25/Out
    1. Exponencial
    2. Funções de Hashing Criptograficas: propriedades, implementação e exemplos
    3. Aplicações: senhas, fingerprint, compromiso, prova de trabalho, encadeamento.
    4. Exercicios: prova de trabalho.
2. 1/Nov
    1. Minieração
    2. Mineração Egoísta
    3. Detecção de Mineração Egoista
    4.
3. 8/Nov
    1. Árvore de Merkle
    2. Problema do Logarimos Discreto
4. 22/Nov
    1. Bitcoin
    2. Pseudo-anonimato
    3. UTxO
5. 29/Nov
    1. Analise de Blockchain
6. 6/Dez
    1. Analise de Blockchain: Exchanges
7. 13/Dez
    1. Analise de Blockchain: Mixers
8. 20/Dez
    1. Analise de Blockchain: Cashing Out
9. 7/Fev
    1. Contratos Inteligentes
10. 14/Fev
    1. Contratos Inteligentes: Segurança
11. 21/Fev
    1. Contratos Inteligentes: Análise de Blockchain
12. 28/Fev
    1. Contratos Inteligentes: Aplicação de protocolos criptográficos
13. 7/Março
    1. Contratos Inteligentes: Aplicação de protocolos criptográficos
14. 14/Março
    1. Avaliação P1
15. 21/Março
    1. Prova de Recuperação

O atendimento aos alunos ocorrerá semanalmente às terças-feiras, entre 20:40 e 22:20. É necessário agendamento prévio pelo chat do MS Teams. O atendimento será realizado na sala do professor, 1B140.

7. AVALIAÇÃO

A avaliação reguar será composta por:

- Prova individual, em 14/Março, com valor de 50 pontos
- Trabalhos diversos com valor de 50 pontos

ATIVIDADE AVALIATIVA DE RECUPERAÇÃO

De acordo com o Art. 141 das Normas de Graduação (Res. CONDIR Nº 46/2022), haverá uma avaliação de recuperação de aprendizagem, que terá valor de 100 pontos. A prova de recuperação abrangerá todo o conteúdo visto no semestre. Ainda, de acordo com o Art. 141, somente fará jus ao direito de realizar a avaliação de recuperação substitutiva o(a) discente que não obtiver o rendimento mínimo de aprovação (60 pontos) e que possuir no mínimo 75% de frequência na disciplina. A nota final após a recuperação será a média da nota obtida durante o semestre e da prova de recuperação.

CONTROLE DE FREQUÊNCIA

A assiduidade será computada através da chamada em sala durante as aulas.

8. BIBLIOGRAFIA

Básica

- Antonopoulos, Andreas. Mastering Ethereum. O'Reilly Media; 1a Edição, 2018. URL = https://github.com/ethereumbook/ethereumbook
- Handbook of applied Cryptography. Alfred J. Menezes, Paul C. Oorschot e Scot A. Vanstone. CRC Press, 1996. URL=https://cacr.uwaterloo.ca/hac/
- Bitcoin and Cryptocurrency Technologies. Narayanan , A et all. Princeton University Press (July 19, 2016). URL= https://bitcoinbook.cs.princeton.edu/

Complementar

- Mastering Bitcoin: Unlocking Digital Cryptocurrencies.Antonopoulos .O'Reilly Media; 1 edition (December 20, 2014) Andreas M.
- Stallings, W. Cryptography and Network Security: Principles and Practice. Prentice-Hall, 2002

- Ferguson, N.; Schneier, B. Practical Cryptography. Wiley Publishing, 2003
- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Singh, Simon. Anchor; (August 29, 2000)
- Handbook of Applied Cryptography - Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone . CRC Press, 2001.

9. APROVAÇÃO

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

Coordenação do Curso de Graduação: _____