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:	Auditoria e Segurança da Informação							
Unidade Ofertante:	Faculdade de Computação							
Código:	GSI035		Período/Série:		8o período		Turma:	S
Carga Horária:						Natureza:		
Teórica:	60	Prática:	0	Total:	60	Obrigatória:	(X)	Optativa: ( )
Professor(A):	Marcelo Keese Albertini					Ano/Semestre:		2023/1
Observações:								

2. EMENTA

Fundamentos de Auditoria de Sistemas de Informações. Auditoria de Sistemas de Informações e de Sistemas em Desenvolvimento. Auditoria de Segurança. Padrões COBIT e ITIL. Controles gerais em ambiente de Tecnologia de Informações. Auditoria de segurança em ambiente de redes e Internet. Certificação de sistemas e de sotware. Introdução à Segurança da informação, Planejamento de Contingência e Continuidade de Negócios, Políticas e Normas em Segurança e Auditoria da Informação, Segurança em Aplicações, Segurança de Operações, Segurança de Redes e Telecomunicações.

3. JUSTIFICATIVA

Segurança da informação, parte integral de Sistemas de Informação, é a atividade de assegurar a proteção de informação em termos de confidencialidade, integridade, disponibilidade e outros requisitos de segurança. 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. A gestão de segurança da informação e auditoria garantem na prática a segurança em ambientes corporativos.

4. OBJETIVO

Objetivo Geral:

Ao término do curso o aluno estará apto a propor ações necessárias para adotar os sistemas de informação de mecanismos de segurança que permitam garantir a integridade e recuperação de informações armazenadas em meio eletrônico.

Objetivos Específicos:

Devem ser desenvolvidas as habilidades:

- conhecimentos dos fundamentos de auditoria de sistemas e Tecnologia da Informação e Comunicação (TIC), conceitos e metodologias para planejar e realizar atividades regulares de mensuração e avaliação de processos, dados, sistemas, infra-estrutura e projetos de TIC;
- capacidade de identificar evidências, causas e consequências de problemas encontrados;
- capacidade de avaliar e recomendar ações de melhoria contínua, com ênfase em controles internos, qualidade e segurança da informação;
- capacidade de descrever e tratar situações reais de trabalhos de auditoria no ambiente de TIC;
- capacidade de fundamentar e apresentar conclusões em relatórios concisos e objetivos de auditoria;
- capacidade de descrever e tratar situações reais de trabalhos de auditoria no ambiente de TIC;

5. PROGRAMA

1. Módulo 1 - Introdução a Conceitos de Segurança da Informação
- Tipos de Ataque
- Serviços e Mecanismos de Segurança
- Criptografia e Criptoanálise

2. Módulo 2 - Algoritmos Simétricos
- Técnicas clássicas
- Block Ciphers (DES)
- Advanced Encryption Standards (AES)
- Modos de operação
- Criptografia Simétrica na Prática

3. Módulo 3 - Algoritmos Assimétricos
- Diffie-Hellman
- RSA
- Curvas elípticas
- Criptografia Assimétrica na Prática

4. Módulo 4 - Autenticidade
- Message Authentication Codes (MAC)
- Algoritmos de Hashing Criptográfico
- Assinaturas Digitais
- Public Key Infraestructure
- Certificados Digitais
- Aplicações Práticas

5. Módulo 5 - Segurança em Ambientes Corporativos
- Normas ISO: 27001 e relacionadas
- Auditoria de Segurança em Sistemas de Informação
- Governança de segurança em sistemas de informação com COBIT/ITIL
- Políticas de Segurança
- Mapeamento de Superfícies de Ataque
- Avaliações de Ameaças de Segurança

6. Módulo 6 - Aspectos Legais
- Legislação Brasileira
- Lei de delitos informáticos 12.737/2012
- Lei Geral de Proteção de Dados

6. METODOLOGIA

A disciplina pede 72 horas-aula.
As aulas serão presenciais em 62 horas-aula de modo expositivo. Haverão 10 horas-aula assíncronas referentes a exercícios.

Os horários de aula são terças-feiras das 20:40 às 22:30 e quartas-feiras das 19:00 às 20:40.

Atendimento com o professor em horário agendado, correio eletrônico albertini@ufu.br ou quartas-feiras das 14h00 às 18h00

O seguinte cronograma será seguido.

	Aulas presenciais	Atividades assíncronas
Aula 01. 01/08 - Introdução à Segurança da Informação	2 horas-aula	
Aula 02. 02/08 - Sistemas criptográficos tradicionais: Ataque à cifra de Vigenère	2 horas-aula	
Aula 03. 08/08 - Sistemas criptográficos tradicionais: modelo de sigilo perfeito e One-Time Pad	2 horas-aula	
Aula 04. 09/08 - Sigilo Computacional	2 horas-aula	
Aula 05. 16/08 - Pseudo Aleatoriedade e Pseudo OTP	2 horas-aula	
Aula 06. 22/08 - Primitivas de segurança: funções e permutações aleatórias	2 horas-aula	
Aula 07. 23/08 - Modelos de ataque: CPA e modos de cifras de bloco	2 horas-aula	
Aula 08. 29/08 - Cifra de bloco: Data Encryption Standard (DES)	2 horas-aula	
Aula 09. 30/08 - Ataque de texto cifrado escolhido: Oráculo de Padding	2 horas-aula	
Aula 10. 05/09 - Advanced Encryption Standard (AES)	2 horas-aula	2 horas-aula para exercícios sobre criptografia simétr
Aula 11. 06/09 - Funções hash criptográficas	2 horas-aula	
Aula 12. 12/09 - Funções hash criptográficas	2 horas-aula	
Aula 13. **13/09 - Prova 1**	2 horas-aula	
Aula 14. 19/09 - Apresentações sobre criptografia simétrica	2 horas-aula	
Aula 15. 20/09 - Apresentações sobre criptografia simétrica	2 horas-aula	
Aula 16. 26/09 - Teoria dos Números: grupos finitos e problemas log-discreto	2 horas-aula	2 horas-aula para exercícios sobre criptografia assim
Aula 17. 27/09 - Introdução criptografia assimétrica	2 horas-aula	
Aula 18. 03/10 - Introdução criptografia assimétrica 2	2 horas-aula	
Aula 19. 04/10 - Esquema de Diffie-Hellman-Merkle	2 horas-aula	
Aula 20. 10/10 - **Reposição de quinta-feira**		2 horas-aula para exercícios sobre criptografia assim
Aula 21. 11/10 - SSL /TLS	2 horas-aula	
Aula 22. 17/10 - Autenticação e não-repudiação: assinaturas eletrônicas	2 horas-aula	
Aula 23. 18/10 - Assinaturas DSA	2 horas-aula	2 horas-aula para exercícios sobre assinatura digital
Aula 24. **24/10 - Prova 2**	2 horas-aula	
Aula 25. 25/10 - Curvas elípticas, Normas ISO 27001	2 horas-aula	2 horas-aula para exercícios sobre uso de criptografia
Aula 26. 31/10 - Normas ISO 27002	2 horas-aula	
Aula 27. 01/11 - Esteganografia, Arquitetura Zero Trust	2 horas-aula	2 horas-aula para exercícios sobre uso de criptografia
Aula 28. 07/11 - Criptografia do Bitcoin,	2 horas-aula	
Aula 29. 08/11 - Lei Geral Proteção de Dados	2 horas-aula	
Aula 30. 14/11 - ISO 27005	2 horas-aula	
Aula 31. **21/11 - Prova de Recuperação**	2 horas-aula	
	60 horas-aula presenciais	12 horas-aula assíncronas

7. AVALIAÇÃO

A avaliação teórica será composta por:

- 2 provas dissertativas sobre o conteúdo ensinado em aula totalizando 60 pontos (prova 1 em 13/09 valendo 30 pontos, prova 2 em 24/10 valendo 30 pontos)
- 2 trabalhos valendo 40 (20+20) pontos

Atividade de recuperação: haverá uma prova de recuperação (sobre todo o conteúdo da disciplina) no dia 21/11/2023 para substituir a nota total (100 pontos).

8. BIBLIOGRAFIA

Básica

- Katz, J. Introduction to Modern Cryptography. 2a edição, 2014.
- Stallings, William. Criptografia e segurança de redes: princípios e práticas. Prentice Hall, 2008.
- Handbook of applied Cryptography. Alfred J. Menezes, Paul C. Oorschot e Scot A. Vanstone. CRC Press, 1996. URL=https://cacr.uwaterloo.ca/hac/
- Guide to Computer Network Security. Joseph Migga Kizza. Springer 2017 URL=http://link.springer.com/openurl?genre=book&isbn=978-3-319-55606-2
- Introductory Computer Forensics. Xiaodong Lin. Springer 2018. URL=http://link.springer.com/openurl?genre=book&isbn=978-3-030-00581-8

Complementar

- Cryptography Made Simple Nigel Smar Springer 2016. URL=http://link.springer.com/openurl?genre=book&isbn=978-3-319-21936-3
- Lyra, Mauricio Rocha; Seguranaça e Auitoria de Sistemas de Informação; Ciência Moderna, 2008. Dias, Claudia;
- Segurança e auditoria da tecnologia da informação; Axcell Books, 2000.
- Segurança de redes : projeto e gerenciamento de redes seguras / Thomas A. Wadlow, Campus 2001
- Security Engineering – Ross Anderson; Wiley, 2001. Firewalls and Internet Security William R. Cheswick and Steven M. Bellovin; Addison- Wesley Professional, 2006.
- Segurança de redes em ambientes cooperativos / Emilio Tissato Nakamura, Paulo Lício de Geus. Editora Novatec, 2007
- Segurança : seu guia para o uso seguro em redes locais / Ed Sawicki ; tradução Jose Paulo T.P. de Faria. - Editora Campus, 1993.
- Redes de computadores : serviços, administração e segurança / Jose Helvecio Teixeira Junior... [et al.]. -. Makron Books 1999.

9. **APROVAÇÃO**

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

Coordenação do Curso de Graduação: _____

Documento assinado eletronicamente por **Marcelo Keese Albertini**, **Professor(a) do Magistério Superior**, em 18/09/2023, às 19:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4701666** e o código CRC **F2865E5B**.

Referência: Processo nº 23117.055173/2023-58 SEI nº 4701666