


UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Computação

Av. João Naves de Ávila, 2121, Bloco 1B - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
 Telefone: (34) 3239-4393 - www.facom.ufu.br - facom@ufu.br


PLANO DE ENSINO
1. IDENTIFICAÇÃO

Componente Curricular:	Segurança da Informação								
Unidade Ofertante:	Facom								
Código:	FACOM32804		Período/Série:		8		Turma:		
Carga Horária:						Natureza:			
Teórica:	60	Prática:	0	Total:	60	Obrigat ória:	(X)	Optativ a:	()
Professor(A):	Ivan da Silva Sendin					Ano/Semestre:		2S2026	
Observações:									

2. EMENTA

2.1. Fundamentos de Auditoria e Segurança de Sistemas de Informação. Propriedades da Informação.

Cópiade Segurança. Introdução a Criptografia. Segurança de Redes. Segurança de Sistemas. Segurança em Aplicações. Planejamento de Conngencia e Connuidade. Auditoria de Segurança. Certificações.

3. JUSTIFICATIVA

3.1. 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 dotar os sistemas deinformação de mecanismos de segurança que propiciem a integridade, disponibilidade e confidencialidade das informações armazenadas em meios eletrônicos.
Objetivos Específicos:
conhecimentos dos fundamentos de auditoria e segurança da informação; capacidade de aplicar os recursos técnicos (segurança de redes, segurança de sistemas) e criptográficos para oferecer segurança da informação; capacidade de identificar evidências, causas e consequências de problema encontrados; capacidade de descrever e tratar situações reais de trabalho de auditoria e segurança no ambiente de TIC; capacidade de fundamentar e apresentar conclusões em relatórios concisos e objetivos de auditoria; capacidade de observar responsabilidades, atitudes e requisitos éticos e conduta do auditor desistemas.

5. PROGRAMA

5.1. Conceitos Básicos

Ameaças nos sistemas de informação

Propriedades da informação

Risco, Impacto e vulnerabilidades

Necessidade de uma Política de Segurança de Informação

5.2. Cópia de Segurança

Política de armazenamento. Disponibilidade. Retenção

5.3. Introdução a Criptografia

Cifradores Clássicos

Ataques Cifradores Modernos

Funções de hashing

Cifradores Assimétricos

Protocolos Criptográficos

5.4. Segurança de Redes

TCP/IP

Firewall

Sistemas de Detecção de Invasão

Outras Ferramentas

5.5. Segurança de Sistemas

Autenticação

Atualização de sistemas

Desenvolvimento de Aplicações

Tratamento de entrada

buffer overflow e similares

5.6. Contigência e Connuidade

Processo de Auditoria

Planejamento de atividades

Avaliação de riscos e vulnerabilidade

Técnicas e Ferramentas

Testes

Relatórios e Recomendações.

6. METODOLOGIA

O curso será ministrado através de aulas expositivas sobre o tema, conforme estabelecido pela coordenação do curso. 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.

O cronograma, que segue a disponibilidade de dias estabelecida pela Resolução CONGRAD Nº 158/2025, é descrito a seguir:

Setembro: 9 Aulas

- 1 - Apresentação da disciplina. Avaliação (REGRAS DA RECUPERAÇÃO) . bibliografia. Visão geral de segurança: Segurança do Wifi, Exponencial e força Bruta
- 2 - CIA - Risco e Impacto
- 8 - Seg redes/Seg Sistemas/Ferramentas: TCP/IP, Ataques, IpSpoofing, DDoS,botnet (colocar ênfase no UDPxTCP)
- 9 - Seg redes/Seg Sistemas/Ferramentas: DNS, firewall, nmap, raw sockets
- 15 - Seg redes/Seg Sistemas/Ferramentas: Scanners, IDS e Sniffing
- 16 - Exercicios
- 22 - Reposição 2a feira
- 23 - Prova P1
- 29 - Cifradores
- 30 - Cifradores: DES, IDEA, OpeanSSL

Outubro 7 Aulas:

- 6 - Hashing
- 7 - Hashing
- 13 - Senhas e Diceware
- 14 - DH/Estabelecimento de chaves
- 20 - Cifradores Assimétricos
- 21 (21 a 24 - TechWeek)
- 27 - Cifradores Assimétricos - Assinaturas
- 28 - Recesso Dia do Servidor

Novembro 8 Aulas:

- 3 Exercicios
- 4 Prova P2
- 10 SSL,PKI e segurança do Wifi
- 11 VPN,TOR e SSL
- 17 Desenvolvimento de Aplicações Seguras
- 18 Desenvolvimento de Aplicações Seguras
- 24 Desenvolvimento de Aplicações Seguras
- 25 Desenvolvimento de Aplicações Seguras

Dezembro 6 Aulas:

- 1 Exercícios
- 2 Prova P3
- 8 Exercícios de Recuperação
- 9 Exercícios de Recuperação
- 15 Exercícios de Recuperação
- 16 Prova de recuperação

O programa contempla 60 horas-aula,as 12 horas aulas restantes serão contempladas com atividades complementares em forma de atividades avaliativas.

O atendimento aos alunos ocorrerá semanalmente às sextas-feiras, entre 8:00 e 10:00 ou em horário de estabelecido de comum acordo. É necessário agendamento prévio por e-mail ou pelo chat do MS Teams. O atendimento será realizado na sala do professor, 1B140 ou pelo próprio chat.

7. AVALIAÇÃO

A avaliação será composta por:

- Prova P1, com 20 pontos
- Prova P2, com 30 pontos
- Prova P3, com 35 pontos
- Trabalhos Diversos: 15 pontos

As datas das provas, estão definidas no item 6 deste documento.

Seguindo as normas estabelecidas pela UFU, serão oferecidas atividades de recuperação - datas no item 6 - com a seguinte pontuação:

- Prova de Recuperação (PRec) 100 pontos
- Trabalho de recuperação(Trec) 5 pontos

A nota final para o aluno que fizer a recuperação será dada por:

$\text{minimo}(60, (NF_{\text{regular}} + 2 \times PRec) / 3 + Trec)$

8. BIBLIOGRAFIA

Básica:

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

Complementar

- 8.5. Cryptography Made Simple Nigel Smar Springer 2016. URL=<http://link.springer.com/openurl?genre=book&isbn=978-3-319-21936-3>
- 8.6. Lyra, Mauricio Rocha; Segurança e Auditoria de Sistemas de Informação; Ciência Moderna, 2008. Dias, Claudia;
- 8.7. Segurança e auditoria da tecnologia da informação; Axcell Books, 2000.
- 8.8. Segurança de redes : projeto e gerenciamento de redes seguras / Thomas A. Wadlow, Campus 2001
- 8.9. Security Engineering – Ross Anderson; Wiley, 2001. Firewalls and Internet Security William R. Cheswick and Steven M. Bellovin; Addison- Wesley Professional, 2006.
- 8.10. Segurança de redes em ambientes cooperativos / Emilio Tissato Nakamura, Paulo Lício de Geus. Editora Novatec, 2007

- 8.11. Segurança : seu guia para o uso seguro em redes locais / Ed Sawicki ; tradução Jose Paulo T.P. de Faria. - Editora Campus, 1993.
- 8.12. 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: _____

Referência: Processo nº 23117.062462/2026-56

SEI nº 7674981