



PLANO DE ENSINO

1. IDENTIFICAÇÃO

Componente Curricular:	GERENCIAMENTO E SEGURANÇA DE REDES						
Unidade Ofertante:	FACULDADE DE ENGENHARIA ELÉTRICA						
Código:	FEELT36802	Período/Série:	8º PERIODO		Turma:	U	
Carga Horária:				Natureza:			
Teórica:	45	Prática:	00	Total:	45	Obrigatória()	Optativa()
Professor(A):	DANIEL COSTA RAMOS				Ano/Semestre:	2026/2	
Observações:							

2. EMENTA

Introdução a Redes Multimídia, Estrutura e Gerenciamento de Redes de Computadores, Introdução à Criptografia de Dados, Segurança de Redes de Computadores e Introdução ao *Software Defined Network*.

3. JUSTIFICATIVA

Capacitar o discente a entender conceitos de ameaças e segurança de redes e a partir dela desenvolver práticas para consolidar seu conhecimento nesta importante área técnica da Telecomunicações e ao mesmo tempo interagir com os serviços e tecnologias de gerenciamento eficiente e seguro de redes.

4. OBJETIVO

Ao final do curso o estudante deverá ser capaz de:

- 1) compreender requisitos para redes multimídia
- 2) configurar e gerenciar os serviços de básicos uma rede de computadores;
- 3) trabalhar com os elementos de segurança de rede implementando seus serviços;
- 4) avaliar parâmetros de segurança e implementar técnicas básicas de proteção de redes de dados.

Entre as competências a serem desenvolvidas no estudante destacam-se:

- 1) Ser capaz de utilizar técnicas adequadas de observação, compreensão, registro e análise das necessidades dos usuários e de seus contextos sociais, culturais, legais, ambientais e econômicos;
- 2) Formular, de maneira ampla e sistêmica, questões de engenharia, considerando o usuário e seu contexto, concebendo soluções criativas, bem como o uso de técnicas adequadas;
- 3) Ser capaz de modelar os fenômenos, os sistemas físicos e químicos, utilizando as ferramentas matemáticas, estatísticas, computacionais e de simulação, entre outras;

- 4) Prever os resultados dos sistemas por meio dos modelos;
- 5) Conceber experimentos que gerem resultados reais para o comportamento dos fenômenos e sistemas em estudo;
- 6) Verificar e validar os modelos por meio de técnicas adequadas;
- 7) Ser capaz de conceber e projetar soluções criativas, desejáveis e viáveis, técnica e economicamente, nos contextos em que serão aplicadas;
- 8) Projetar e determinar os parâmetros construtivos e operacionais para as soluções de Engenharia;
- 9) Ser capaz de expressar-se adequadamente, seja na língua pátria ou em idioma diferente do Português, inclusive por meio do uso consistente das tecnologias digitais de informação e comunicação (TDICs), mantendo-se sempre atualizado em termos de métodos e tecnologias disponíveis;
- 10) Aprender a aprender.

5. PROGRAMA

1. Introdução a Redes Multimídia

- 1.1 Aplicações de redes multimídia
- 1.2 Vídeo de fluxo contínuo e VoIP
- 1.3 Protocolos para aplicações interativas em tempo real
- 1.4 Suporte de rede para multimídia

2. Estrutura e Gerenciamento de Redes de Computadores

- 2.1 Arquitetura e Requisitos
- 2.2 Infraestrutura de Rede
- 2.3 Protocolos
- 2.4 Modelo TMN
- 2.5 Gerenciamento Remoto

3. Introdução à Criptografia de Dados

- 3.1 Apresentação, histórico e importância da codificação de informações
- 3.2 Criptografia Simétrica
- 3.3 Criptografia Assimétrica

4. Segurança de Redes de Computadores

- 4.1 O problema da segurança de redes públicas
- 4.2 Tipos de ataques em redes de computadores
- 4.3 *Firewalls*
- 4.4 Detecção e prevenção de invasões
- 4.5 Segurança de redes Wireless
- 4.6 Segurança na camada de Transporte
- 4.7 Segurança na camada de rede: IPsec e redes virtuais privadas
- 4.8 Segurança na Nuvem

5. Introdução ao *Software Defined Network*

- 5.1 Introdução e conceitos básicos

6. **METODOLOGIA**• **Conteúdo Programático para Atividades Teóricas Presenciais**

As aulas teóricas serão realizadas às quintas-feiras das 09h50min às 12h20min no Bloco G da UNIPAM, sala 403.

Aula	Data	Conteúdo Teórico	Subtópicos Previstos
01-02-03	03/09	Apresentação da disciplina Fundamentos e Arquitetura de Redes de Computadores	Arquiteturas e componentes de rede; LAN, WAN e Internet; revisão de Ethernet, ARP, IP, ICMP, TCP e UDP; DNS e DHCP; portas e serviços; encapsulamento;
04-05-06	10/09	Estrutura e Gerenciamento de Redes	Objetivos do gerenciamento; inventário e documentação; disponibilidade e desempenho; NMS; gerente, agente e dispositivo gerenciado; gerenciamento centralizado; gerenciamento in-band e out-of-band; modelo FCAPS; introdução ao modelo TMN e seus níveis.
07-08-09	17/09	Monitoramento e Desempenho de Redes	Monitoramento ativo e passivo; SNMP; MIB e OID; polling e traps; SNMPv2c e SNMPv3; Syslog; NTP; disponibilidade, latência, perda, jitter, vazão e utilização; baseline e limiares; breve relação com VoIP, streaming e QoS.
10-11-12	24/09	Gerenciamento Remoto e Administração Segura	Administração local e remota; Telnet e SSH; autenticação por senha e chaves; usuários e privilégios; AAA; RADIUS e TACACS+; princípio do menor privilégio; backup e atualização de configurações; hardening; introdução a APIs, NETCONF e YANG.
13-14-15	01/10	Fundamentos de Segurança da Informação e Ameaças em Redes	Confidencialidade, integridade e disponibilidade; ativo, ameaça, vulnerabilidade, risco e controle; controles preventivos, detectivos e corretivos; defesa em profundidade; princípio do menor privilégio; introdução à ISO/IEC 27001 e ABNT NBR ISO/IEC 27002; reconhecimento, scanning, sniffing, spoofing, ataques a credenciais, MITM, DoS/DDoS e exploração de vulnerabilidades.
16-17-18	08/10	Introdução à Criptografia de Dados (Seminário)	Conceitos e breve histórico; codificação × criptografia; criptografia simétrica; AES como exemplo; hashes e integridade; HMAC; armazenamento de senhas e salt; criptografia assimétrica; chaves pública e privada; assinatura digital; certificados digitais; autoridades certificadoras; PKI; introdução ao TLS.
-	15/10	*REPOSIÇÃO DE SEGUNDA	*REPOSIÇÃO DE SEGUNDA
19-20-21	22/10	Avaliação 1	Avaliação 1

22-23-24	29/10	Firewalls e Segmentação de Redes	Políticas de segurança; ACLs; firewalls stateless e stateful; filtragem por endereço, protocolo e porta; políticas default allow e default deny; NAT/PAT; segmentação; VLANs; zonas de segurança; DMZ; princípio do menor privilégio e defesa em profundidade.
25-26-27	05/11	Deteção, Prevenção e Monitoramento de Segurança	IDS e IPS; NIDS e HIDS; detecção por assinatura e anomalia; falso positivo e falso negativo; eventos, alertas e incidentes; logs; correlação; introdução a SIEM; análise básica de tráfego e PCAP; fundamentos de resposta a incidentes.
28-29-30	12/11	Segurança na Camada de Transporte e Redes Privadas Virtuais	TLS e HTTPS; autenticação e estabelecimento de conexão segura; conceito de túnel; VPN de acesso remoto e site-to-site; IPsec; AH e ESP; modos transporte e túnel; IKE em nível conceitual; WireGuard (exemplo).
31-32-33	19/11	Segurança em Redes Sem Fio	Fundamentos de WLAN; AP, SSID e BSSID; canais e interferência; autenticação e associação; WEP, WPA, WPA2 e WPA3; PSK e Enterprise; 802.1X e RADIUS; WPS; rogue AP; evil twin; ataques de desautenticação em nível conceitual; isolamento de clientes; redes de visitantes; segurança e troubleshooting wireless.
34-35-36	26/11	Segurança em Nuvem (Seminário)	IaaS, PaaS e SaaS; modelo de responsabilidade compartilhada; redes virtuais; VPC/VNet; sub-redes públicas e privadas; security groups; IAM; usuários, papéis e permissões; princípio do menor privilégio; proteção de dados em trânsito e em repouso; exposição de serviços; logs e monitoramento; segurança de arquiteturas híbridas.
37-38-39	03/12	SDN, Gerenciamento Programável e Integração dos Conteúdos	Limitações do gerenciamento tradicional dispositivo a dispositivo; planos de dados, controle e gerenciamento; arquitetura SDN; controlador SDN; interfaces northbound e southbound; OpenFlow em nível introdutório; APIs e automação; aplicações de SDN em gerenciamento e segurança. Integração dos conteúdos da disciplina por meio de troubleshooting de um caso exemplo.
40-41-42	10/12	Avaliação 2	Avaliação 2
43-44-45	17/12	Recuperação	Recuperação

• Conteúdo Programático para Atividades Acadêmicas Extras

Aula	Data	Conteúdo Teórico
01-02-03	01/10	Preparação para Seminário
04-05-06	12/11	Preparação para Seminário
07-08-09	19/10	Preparação para Seminário

• **Resumo da Carga Horária**

Carga Horária	Teórica
Presencial Total	45
AAE Total	09
Total da disciplina	54

• **Atendimento**

O atendimento aos alunos da disciplina será realizado de forma presencial no Bloco Alfa, sala 312, de acordo com o seguinte planejamento: segundas-feiras entre 15h00 e 16h00, ou outro dia desde que agendado com o professor previamente.

7. **AVALIAÇÃO**

• **Aproveitamento**

A avaliação de desempenho dos discentes será feita por entrega de estudos dirigidos, apresentação de seminários e duas provas. O cronograma de atividades avaliativas e a distribuição da pontuação é apresentada.

Os resultados das avaliações serão divulgados no mural do curso, sendo que as notas serão apresentadas pelos números de matrícula dos alunos. A divulgação das notas deve acontecer em até 15 dias úteis após a sua realização e a vista de prova será marcada com os alunos, a partir da data de divulgação das notas, respeitando-se o prazo de no máximo 5 dias úteis, como previsto na Resolução do CONGRAD (Nº46/2022).

DATA	ATIVIDADE AVALIATIVA	PONTUAÇÃO
-	% de Presença	10 pontos
08/10 26/11	Seminários	40 pontos
22/10	Avaliação 1	25 pontos
10/12	Avaliação 2	25 pontos
TOTAL		100 pontos

• **Frequência**

A frequência para aulas presenciais será aferida por chamada oral durante as aulas.

• **Recuperação**

É necessário ter 75% de presença para ter direito a realizar a prova de recuperação e a mesma somente será aplicada para o aluno que não atingiu 60 pontos.

A recuperação consistirá de uma avaliação no valor de 100 pontos, presencial e individual. Não será permitido consulta. Será permitido o uso de calculadoras. Celulares deverão ser desligados durante a avaliação. A recuperação não terá

nenhuma questão que utilize simulação.

Considerando a Média Final Parcial (MP) a nota obtida no semestre ante da recuperação e a Recuperação (REC) como acima descrita, a Nota Final da disciplina (MF) será dada pela seguinte fórmula:

$$MF = (MP)*0,5 + (REC)*0,5, \text{ sendo limitado em 60 o valor máximo de MF obtido pelo aluno em recuperação.}$$

8. BIBLIOGRAFIA

Básica

1. KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem top-down 6.ed. São Paulo: Pearson Education do Brasil, 2013.
2. SIQUEIRA, L. A. **Infraestrutura de redes**. Elsevier, 2013.
3. STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson Education do Brasil, 2014.
4. TANENBAUM, A. S. **Redes de computadores**. 5.ed. São Paulo: Pearson Education, 2011.

Complementar

1. COLLINS, M. **Network Security Through Data Analysis**: Building Situational Awareness. 1 ed. O'Reilly Media, 2014.
2. KARL, H.; WILLING, A. **Protocols and Architectures for Wireless Sensor Networks**. 1 ed. Wiley, 2007.
3. MARIN, Paulo S. **Cabeamento estruturado**. 1ed. São Paulo: Érica, 2014. Disponível em <https://www.sistemas.ufu.br/biblioteca-gateway/minhabiblioteca/9788536533124>.
4. STALLINGS, W. **Network security essentials**: applications and standards. 2nd ed. Upper Saddle River: Prentice Hall, 2002.
5. SOUSA, L. B. **Administração de redes locais**. 1ed. São Paulo: Érica, 2014.

9. APROVAÇÃO

Aprovado em reunião do Colegiado conforme Decisão Administrativa do Colegiado anexada ao processo referenciado.

Coordenação do Curso de Graduação: _____



Documento assinado eletronicamente por **Daniel Costa Ramos**, **Coordenador(a)**, em 07/10/2026, às 07:57, 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 **7557523** e o código CRC **7F6BC0D4**.